Sensor Network Security: A Survey

Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou

***Abstract*—Wireless sensor networks (WSNs) use small nodes with constrained capabilities to sense, collect, and disseminate information in many types of applications. As sensor networks become wide-spread, security issues become a central concern, especially in mission-critical tasks. In this paper, we identify the threats and vulnerabilities to WSNs and summarize the defense methods based on the networking protocol layer analysis first. Then we give a holistic overview of security issues. These issues are divided into seven categories: cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other security issues. Along the way we analyze the advantages and disadvantages of current secure schemes in each category. In addition, we also summarize the techniques and methods used in these categories, and point out the open research issues and directions in each area.**

***Index Terms*—Sensor networks, Security, Ad hoc networks, Survey, key management, Attack detections and preventions, Secure routing, Secure location, Secure data aggregation, Node compromise.**

I. Introduction

FOLLOWING the recent advances in micro-electro-mechanical systems (MEMS) [1]-[4] technology, wireless communications, and digital electronics, it is technically and economically practical to manufacture a large number of small and low cost sensors. These tiny sensor nodes consist of sensing, data processing, and communicating components. It is possible to deploy these sensor nodes inside or close to the inspected phenomenon, and to organize them as a wireless sensor network (WSN) or sensor network. Sensor networks may consist of many different types of sensors, such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic, and radar, which can monitor temperature, humidity, vehicular movement, lighting condition, pressure, soil makeup, noise levels, etc. [1]. Because of this, they have a wide range applications. Akyildiz, et al. [5] classify the applications of sensor networks as military applications, environmental applications, health applications, home applications, and other commercial applications.

Many sensor networks have mission-critical tasks, such as above military applications, thus it is clear that security needs to be taken into account at the time of design. While WSNs come from wireless ad hoc networks, important distinctions exist between them and these differences greatly affect the system designs including security designs. The differences are as the following [6]:

- Compared with ad hoc nodes, sensor nodes are limited in computation, memory, power resources, and communication speed or bandwidth.
- Sensor nodes may not have global identification.
- Compared with ad hoc nodes, a WSN normal has one base station, which has more computing capabilities and assumes the controller of the network.
- Compared with ad hoc nodes, sensor nodes are prone to failures due to harsh deployment environments and energy constraints.
- Compared with ad hoc nodes, sensor nodes are easy to be compromised.
- The topology of a WSN changes very frequently due to the node failure, joining or mobility.
- Sensor nodes are densely deployed in most environments.
- Compared with ad hoc nodes, the number of nodes in a WSN can be several orders of magnitude higher than the nodes in an ad hoc network.

Due to such differences and difficulties, security in WSNs is more complicated, thus introducing more studies to address the security issues. In this paper, we identify the threats and vulnerabilities to sensor networks and summarize the defense methods based on the networking protocol layer analysis. Then we explore current proposals in sensor network security that have been developed over the period after 2000, and develop a classification for these studies. Our objective is to provide a deeper understanding of current security approaches in WSNs, and to identify some open research issues that can be further pursued. A few existing surveys on security issues in WSNs can be found [7], [8]. However, these articles do not discuss secure location issues and other security issues such as security-energy assessment, data assurance, survivability, etc., which are also important to secure WSNs. Further, our paper includes a large number of recent available literatures on security in WSNs.

The remainder of the proposal is organized as follows: Background information on WSNs including security goals, challenges, threats and attacks, and evaluation is presented in Section II. Section III gives a short summation of security issues and defense suggestions from the point of view of OSI model. Then we focus on the security issues and solutions in seven categories: cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other security issues from Section 4 to Section 10. Finally, we summarize this paper.

Manuscript received 12 March 2007; revised 14 April 2008.

The authors are with the Telecommunication and Information Technology Institute, Florida International University (e-mail: fuqiang_chen178@hotmail.com).

Digital Object Identifier 10.1109/SURV.2009.090205.

1553-877X/09/$25.00 © 2009 IEEE

II. Background

A. Security Goals

When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services:

- Confidentiality: Confidentiality or Secrecy has to do with making information inaccessible to unauthorized users [9], [10]. A confidential message is resistant to revealing its meaning to an eavesdropper.
- Availability: Availability ensures the survivability of network services to authorized parties when needed despite denial-of-service attacks. A denial-of-service attack could be launched at any OSI (Open System Interconnect) layer [9] of a sensor network.
- Integrity: Integrity measures ensure that the received data is not altered in transit by an adversary [9], [10].
- Authentication: Authentication enables a node to ensure the identity of the peer node with which it is communicating [9], [10].
- Non-repudiation: Non-repudiation denotes that a node cannot deny sending a message it has previously sent.
- Authorization: Authorization ensures that only authorized nodes can be accessed to network services or resources.
- Freshness: This could mean data freshness and key freshness. Since all sensor networks provide some forms of time varying measurements, we must ensure each message is fresh. Data freshness implies that each data is recent, and it ensures that no adversary replayed old messages.

Moreover, as new sensors are deployed and old sensors fail frequently in WSNs, the following forward and backward secrecy are also important to security:

- Forward secrecy: a sensor should not be allowed to know future messages after it leaves the network.
- Backward secrecy: a newly joining sensor should not be able to know any previously transmitted message.

B. Security Challenges

We summarize security challenges in sensor networks from [6], [11], [12] as follows:

- Minimizing resource consumption and maximizing security performance.
- Sensor network deployment renders more link attacks ranging from passive eavesdropping to active interfering.
- In-network processing involves intermediate nodes in end-to-end information transfer.
- Wireless communication characteristics render traditional wired-based security schemes unsuitable.
- Large scale and node mobility make the affair more complex.
- Node adding and failure make the network topology dynamic.

C. Threats and Attacks

Security issues mainly come from attacks. Base stations in WSNs are usually regarded as trustworthy. Most research studies focus on security issues among sensor nodes. If no attack occurred, there is no need for security. Generally, the attack probability within sensor networks is larger than that of any other types of networks, such as wireless LANs, due to their deployment environments and resource limitations [6]. These attacks can be classified as external attacks and internal attacks. In an external attack, the attacker node is not an authorized participant of the sensor network [6]. External attacks can further be divided into two categories: passive and active. Passive attacks involve unauthorized ‘listening’ to the routing packets. This type of attack can be eased by adopting different security methods such as encryption. Active external attacks disrupt network functionality by introducing some denial-of-service (DoS) attacks, such as jamming, power exhaustion. Authentication and integrity will ease most active external attacks except jamming. The standard defense against jamming involves various forms of spread-spectrum or frequency hopping communication. Other defense methods against jamming include switching to low duty cycle and conserving as much power as possible, locating the jamming area and rerouting traffic, adopting prioritized transmission scheme that minimize collisions, etc. [13].

Node compromise is the major problem in sensor networks that leads to internal attacks. With node compromise, an adversary can perform an internal attack. In contrast to disabled nodes, compromised nodes actively seek to disrupt or paralyze the network [6]. Normally, compromised nodes can be obtained by the following methods:

- Attackers capture sensor nodes and reprogram them. The advantage of this method is quick and easy. But this method has some limitations. Firstly, it is not easy to capture and reprogram sensor nodes automatically. Most time, attackers must manually capture nodes and reprogram them. Secondly, in some applications, the deployment environment makes it difficult or even impossible for attackers to capture sensor nodes, e.g. some military applications. Thirdly, WSNs can locate the compromised nodes by monitor node activity, location, etc. [14].
- Attackers can deploy nodes with larger computing resources such as laptops to attack sensor nodes. For example, laptop attackers’ nodes can communicate sensor nodes, breach their security mechanisms, insert malicious codes and make them as compromised nodes without physically touching them or moving their positions. These laptop nodes compromising activities can execute at all time, and these compromise activities are hard to be detected, and can be implemented automatically. The disadvantage is that attackers need some time to breach security mechanisms of sensor nodes.
- Attackers can deploy big nodes as compromised nodes. Attackers can deploy big nodes such as laptop nodes as compromised nodes to replace current sensor nodes when they get the secret information by attacking normal nodes. Similar to the above case, it is hard for detecting mechanisms to detect such compromised nodes. The disadvantages of this method are: attacking time is a little longer compared with the first introduced method; the cost is expensive when using one laptop as one node. Someone may say that attacker can use one laptop to forge several nodes. This type of attack is Sybil attack

[15]. System can easily locate them by using Location Verification, Identity Verification [15].

Compared with external attacks, internal attacks are hard to be detected and prevented, thus raising more security challenges. Compromised nodes can do the following attacks:

- Compromised node can steal secrets from the encrypted data which passed it;
- Compromised node can report wrong information to the network;
- Compromised node can report other normal nodes as compromised nodes;
- Compromised node can breach routing by introducing many routing attacks, such as selective forwarding, black hole, modified the routing data, etc., while systems are hard to notice these activities, and normal encryption methods have no effect to prevent them because they own the secret information such as keys;
- Compromised nodes may exhibit arbitrary behavior and may collude with other compromised nodes.

D. Evaluation

Besides implementing the security goal discussed above, the following metrics are also important to evaluate whether a security scheme is appropriate for WSNs [7], [8].

- Resiliency: Resilience is the ability of the network to provide and maintain an acceptable level of security service in case some nodes are compromised.
- Resistance: Resistance is the ability to prevent the adversary from gaining full control of the network by node replication attack [16] in case some nodes are compromised.
- Scalability, self-organization and flexibility: In contrast to general ad hoc networks that do not put scalability in the first priority, designing sensor network must consider its scalability because of its large quantity of sensor nodes. Due to its deployment condition and changeable mission goals, self-organization and flexibility (such as sensor networks fusing, nodes leaving and joining, etc.) are also important factors when designing secure sensor network.
- Robustness: A security scheme is robust if it continues to operate despite abnormalities, such as attacks, failed nodes, etc.
- Energy efficiency: A security scheme must be energy efficient so as to maximize network lifetime.
- Assurance: It is an ability to disseminate different information at different assurance levels to the end-user [17]. A security scheme had better allow a sensor network to deliver different level information with regard to different desired reliability, latency, etc. with different cost.

III. Attacks and Defense Suggestions in OSI Model

Here we give a short summation of security issues and defense suggestions from the point of view of Open System Interconnect (OSI) model. Using layered network architecture can help to analyze security issues, and improve robustness by circumscribing layer interactions and interfaces. Fig. 1 is the typical layered networking model of a sensor network. Each layer is susceptible to different attacks. Even some attacks can crosscut multiple layers or exploit interactions between them. In this section, we mainly discuss attacks and defenses on the transport layer and the below layers.

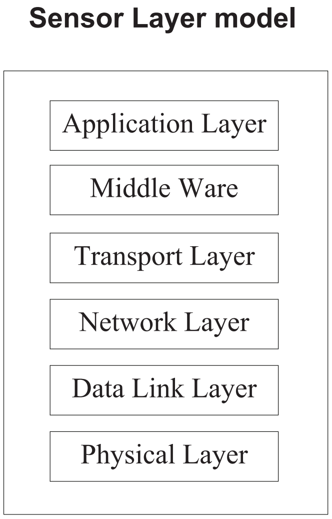

Fig. 1. Layered networking model of sensor network.

A. Physical Layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection and modulation [5]. Jamming and tampering are the major types of physical attacks. The standard defense against jamming involves various forms of spread-spectrum or frequency hopping communication. Given that these abilities require greater design complexity and more power, low-cost and low-power sensor devices will likely be limited to single-frequency use [13]. Other defense methods against jamming include switching to low duty cycle and conserving as much power as possible, locating the jamming area and rerouting traffic, adopting prioritized transmission schemes that minimize collisions, etc. Capturing and tampering is one of methods that produce compromised nodes. An attacker can also tamper with nodes physically, interrogate and compromise them. Tamper protection falls into two categories: passive and active [11]. Passive mechanisms include those that do not require energy and include technologies that protect a circuit from being detected (e.g., protective coatings, tamper seals). Active tamper protections involve the special hardware circuits within the sensor node to prevent sensitive data from being exposed. Active mechanisms will not be typically found in sensor nodes since these mechanisms add more cost for extra circuitry and consume more energy. Instead, passive techniques are more indicative of sensor node technology.

B. Data Link Layer

The data link layer or media access control (MAC) is responsible for the multiplexing of data streams, data frame detection, medium access and error control [5]. It provides reliable point-to-point and point-to-multipoint connections in a communication network, and channel assignment for neighbor-to-neighbor communication is a main task for this layer. Collision, exhaustion, and unfairness are major attacks in this layer. Error-correcting code can ease collision attack, however, the result is limited because malicious nodes can still corrupt more data than the network can correct. Also, the collision-detection mechanism cannot completely defend against that attack because proper transmission still need cooperation among nodes and subverted nodes could intentionally and repeatedly deny access to the channel, expending much less energy than in fulltime jamming [13]. TDMA is another method in preventing collisions. But it requires more control resources and is still susceptible to collisions. Adversaries can let sensor nodes execute a large number of tasks to deplete the battery of these nodes. This exhaustion attack will compromise the system availability even if the adversary expends few efforts. Random back–offs only decrease the probability of an inadvertent collision, thus they would be ineffective at preventing this attack. Time-division multiplexing gives each node a slot for transmission without requiring arbitration for each frame. This approach could solve the indefinite postponement problem in a back–off algorithm, but it is still susceptible to collisions. A promising solution is rate limiting in MAC admission control, but it still needs additional work [13]. In a non-priority MAC mechanism, adversaries can adopt maximizing their own transmission time in order to let the other good nodes not have any time to transmit packets. This will cause unfairness, a weaker form of DoS. Though this threat may not entirely prevent legitimate access to the channel, it could degrade normal service. Though using small frames can ease some extents of such attacks, it increases framing overhead when the network typically transmits long messages. Further, an adversary can easily defeat this defense by cheating when vying for access, such as by responding quickly while others delay randomly [13].

C. Network Layer

Sensor nodes are scattered in a field either close to or inside the phenomenon [5]. Special multihop wireless routing protocols between the sensor nodes and the sink node are needed to deliver data throughout the network. Karlof and Wagne [18] summarize the attacks of the network layer as follows: Spoofed, altered, or replayed routing information; Selective forwarding; Sinkhole attacks; Sybil attacks; Wormholes; HELLO flood attacks; and acknowledgement spoofing.

- **Countermeasure summary in Network layer**

Encryption and authentication, multipath routing, identity verification, bidirectional link verification, and authentication broadcast can protect sensor network routing protocols against external attacks, bogus routing information, Sybil attacks, HELLO floods, and acknowledgement spoofing. Sinkhole attacks, and wormholes pose significant challenges to secure routing protocol design, especially integrating node compromise. It is unlikely to find effective countermeasures against these attacks that can be applied after deployment. It is crucial to design routing protocols in which these attacks are meaningless or ineffective. Geographic routing protocols are one class of protocols that holds promise [18].

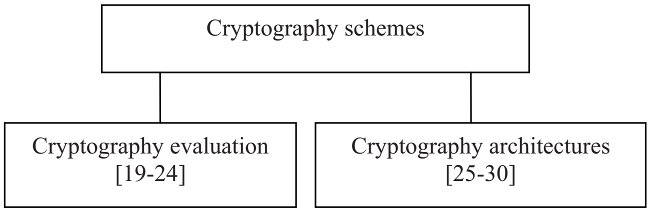
Cryptography schemes
Cryptography evaluation [19-24]
Cryptography architectures [25-30]

Fig. 2. Taxonomy of cryptography schemes.

D. Transport Layer

The transport layer protocols provide reliability and session control for sensor node applications [5]. This layer is especially needed when the system plans to be accessed through Internet or other external networks. Though it is considered to have few security issues in this layer, there are still some types of attacks, such as flooding and desynchronization that can threaten the security. Though limiting the number of connections can prevents flooding, it also prevents legitimate clients from connecting to the victim as queues and tables filled with abandoned connections. Protocols that are connectionless, and therefore stateless, can naturally resist this type of attack somewhat, but they may not provide adequate transport-level services for the network. Solving client puzzles can partially ease this type of attack [13]. Desynchronization can disrupt an existing connection between two endpoints. In this attack, the adversary repeatedly forges messages carrying sequence numbers or control flags, which cause the endpoints to request retransmission of missed frames to one or both endpoints. One counter to this attack is to authenticate all packets exchanged, including all control fields in the transport protocol header. The endpoints could detect and ignore the malicious packets, supposing that the adversary cannot forge the authentication message [13].

IV. Cryptography

A. State-of-the-Art

Cryptography is the basic encryption method used in implementing security. Symmetric key cryptography uses the same key for encryption and decryption. Another type of encryption method, asymmetric or public key cryptography uses different keys to encrypt and decrypt. On one hand, asymmetric key cryptography (e.g., the RSA signature algorithm) requires more computation resources than symmetric key cryptography (e.g., the AES block cipher) does, on the other hand, symmetric key cryptography is difficult for key deployment and management. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated before choosing. In this section, we focus on cryptography evaluations and cryptography architectures. Fig. 3 shows the taxonomy of cryptography.

1) Cryptography Evaluations: To evaluate the computational overhead of cryptographic algorithms, Ganesan, et al. in [19] chose RC4, IDEA, RC5, MD5 and SHA1 as the popular symmetric encryption and hashing function schemes. They did a series performance evaluation experiments for these choosing algorithms based on different hardware platforms including Atmega 103, Atmega 128, M16C/10, SA-1110, PXA250 and UltraSparc2. Experimental measurements

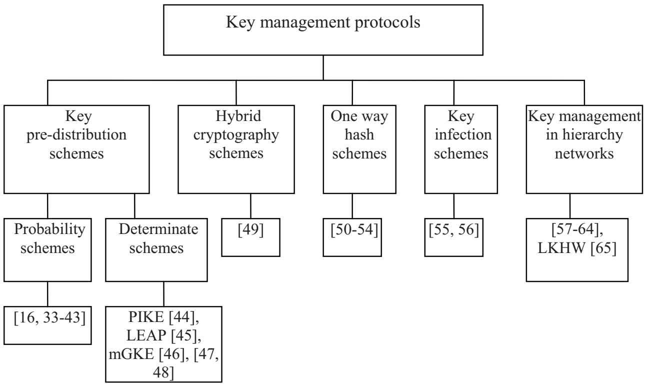

Fig. 3. Taxonomy of key management protocols.

indicate uniform cryptographic cost for each encryption class and each architecture class and negligible impact of caches. RC4 is shown to outperform RC5 for the Motes Atmega platform contrary to the choice of RC5 for the Motes project [20], a choice driven in large by memory constraints. From the findings and the experimental data, they derived a model that allows the interpolation of performance for other architectures. Their model assesses the impact of arbitrary embedded architectures as a multi-variant function for each encryption scheme depending on processor frequency, word width, ISA type and specific ISA support.

Law, et al. [21], [22] propose their own systematic framework that considers both the security properties and the efficiencies of storage and energy in order to evaluate and assess these candidates. They compare several ciphers such as RC5, RC6, Rijndael, MISTY1, KASUMI, and Camellia and conclude that Rijndael is the suitable cipher when considering security and energy efficiency for sensor networks, and MISTY1 is a good selection when considering storage and energy efficiency.

Several public key system costs are compared by Malan in [23] in terms of transmission time, round trip time, computation overhead, memory overhead, etc. The research shows: SKIPJACK is reasonable; Diffie-Hellman (DLP) is respectable and still has room for optimization though the key sizes are unappealing; the key size of Elliptic Curve Diffie-Hellman (ECDLP) is appealing and has potential though it still need some works to optimize. The research work of Gaubatz, et al. in [24] shows PKC is acceptable in sensor networks.

2) Cryptography Architectures: Some researchers implement cryptography with software in normal sensor networks' hardware. For example, Malan, et al. [25] propose the first known implementation of elliptic curve cryptography for sensor networks based on the 8-bit, 7.3828-MHz MICA2 [31] mote. Others implement cryptography with specific cryptography design in hardware such as [26]. Some approaches are based on symmetric cryptography, while others use asymmetric cryptography or both. Most asymmetric cryptography architectures [27, 28] balance the overheads between sensors and base stations. Some approaches adopt both asymmetric and symmetric cryptography to ease the overheads. For example, a security architecture proposed by Schmidt, et al. in [29] includes three different interacting phases: a pairwise key agreement to provide authentication and the initial key exchange, the establishment of sending clusters to extend pairwise communication to broadcast inside the communication range, and encrypted and authenticated communication of sensor data. Some approaches such as Yuksel, et al. in [30] propose variations of universal hash function to adapt to sensor network environment.

B. Summary

Cryptography selection is fundamental to providing security services in WSNs. Many researchers consider that public key cryptography schemes are not suitable for WSNs due to the resource limitation of sensor nodes. Although some recent research results show that it is feasible to apply public key cryptography to WSNs by choosing appropriate algorithms, parameters, etc., private key operations in asymmetric cryptography schemes are still too expensive in terms of computation and energy cost for sensor nodes, and still need further studies. Symmetric key cryptography is superior to public key cryptography in terms of speed and low energy cost. However, the key management is not an easy task for symmetric key cryptography. Efficient and flexible key management schemes need to be designed.

V. Key Management

A. State-of-the-Art

Considering security, key management is very important and complex especially in symmetric cryptography structure. Sensor network dynamic structure, easy node compromise and self organization property increase the difficulty of key management and bring a broad research issues in this area.

Due to the importance and difficulty of key management in WSNs, there are a large number of approaches focused on this area. Based on the main technique that these proposals used or the special structure of WSNs, we classify the current proposals as key pre-distribution schemes, hybrid cryptography schemes, one way hash schemes, key infection schemes, and key management in hierarchy networks, though some schemes combine several techniques. An existing survey on key management in WSNs can be found in [32]. However, the article does not discuss Key infection schemes. Fig. 4 shows the taxonomy of key management.

1) Key Pre-Distribution Schemes: In the key predistribution schemes, sensor nodes store some initial keys before they are deployed. After deployed, the sensor nodes can use the initial keys to setup secure communication. This method can ease key management especially for sensor nodes that have limited resource. Thus many approaches adopt key pre-distribution method. In addition, in these approaches, the communications between the base station and sensors are smaller compared with centralized approaches, thus the base station is not a bottleneck problem. So, we not only call it key pre-distribution management, but also distributed key management. A naive solution is to let all the nodes to carry a master secret key. Any pair of nodes can use this global master secret key to initiate key management. The advantage of this scheme is that it only needs store one master key in a node before its deployment. However, if one

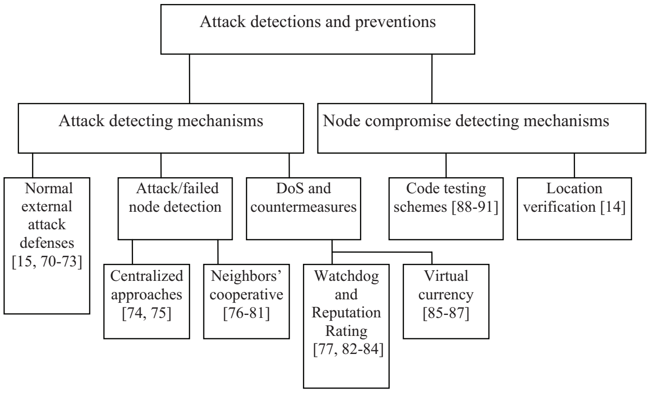
Attack detections and preventions
Attack detecting mechanisms
Node compromise detecting mechanisms
Normal external attack defenses [15, 70-73]
Attack/failed node detection
DoS and countermeasures
Code testing schemes [88-91]
Location verification [14]
Centralized approaches [74, 75]
Neighbors' cooperative [76-81]
Watchdog and Reputation Rating [77, 82-84]
Virtual currency [85-87]

Fig. 4. Taxonomy of attack detections and preventions.

node is compromised, the security of the whole network will be compromised. Some existing studies suggest storing the master key in tamper-resistant hardware to make the system more secure, but it is impractical to implement such equipment in sensor nodes. Furthermore, tamper-resistant hardware might also be conquered [66]. Another normal key pre-distribution scheme is to let each sensor store N-1 secret pairwise keys, each pairwise key is only known to this sensor and one of the other N-1 sensors (assuming N is the total number of sensors). Though compromising one node does not affect the security of the other nodes, this scheme is impractical for current generation sensor with an extremely limited amount of memory because N could be large. Moreover, it is difficult for new nodes to join in a pre-existing sensor network because the currently deployed nodes do not have pairwise keys with new added sensors.

In some key pre-distribution schemes, the existence of a shared key between a particular pair of nodes is not certain but is instead guaranteed only probabilistically; while other approaches guarantee that any two nodes can be able to establish a key. Thus, we classify key pre-distribution schemes as probability schemes and determinate schemes.

- **Probability schemes**

We classify some proposals of key management as probability schemes when the existence of one or more common predistribution keys between intermediate nodes is not certain but is instead guaranteed only probabilistically. The basic idea of these schemes is to randomly preload each sensor with a subset of keys from a global key pool before deployment. Thus, we also call them random key predistribution (RKP) schemes.

The basic probabilistic key pre-deployment scheme is introduced by Eschenauer and Gligor in [33]. Their scheme consists of three phases: key pre-distribution, shared-key discovery, and path-key establishment. The main contribution of this paper is that: randomly drawing a small number of keys from a large key pool and storing in each sensor node can obtain a considerably large probability that two neighbor nodes will have a shared key.

Based on the Eschenauer-Gligor scheme, some researchers provide key pre-distribution schemes that improve the network resilience to prevent node compromise. Chan, et al. propose a q-composite random key pre-distribution scheme [16]. Different from Eschenauer-Gligor scheme that only needs 1 common key, their scheme requires q common keys $(q \geq 1)$ to establish secure communications between a pair of nodes. And they show that when q is increased, the network resilience against node compromise is improved, i.e., attackers need compromise more nodes to achieve a high probability of compromised communication. Of course, when q is increased, the sensor nodes should store more pre-distribution keys in order to obtain an applicable probability of key-shared within neighbors. Du, et al. [34] propose a key predistribution scheme with a definite node compromise threshold λ, which improves the resilience of the network. This scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold λ, the probability that any nodes other than these compromised nodes are affected is near to zero. This desirable property makes it necessary for the adversary to attack a significant proportion of the network in order to breach the network when the security designers elaborately select the λ. Liu and Ning [35] develop a similar method. The key difference between [34] and [35] is that the scheme in [35] is based on a set of bivariate t-degree polynomials while scheme in [34] is based on Blom's method [67]. Different from scheme in [35] using bivariate polynomials, scheme in [36] uses multivariate polynomials and it also provide threshold feature.

Based on the combination of probabilistic key sharing and threshold secret sharing schemes, Zhu, et al. [37] present an approach for establishing a pairwise key that is exclusively known to a pair of nodes with overwhelming probability. They implement a secure pairwise key between any pair of nodes by splitting the key into multiple shares and transmitting these shares into different paths and cooperating them to reconstruct it. Another type of probabilistic model to establish pair-wise key scheme proposed by Pietro, et al. in [38] use pseudo-random, seed-based technique. Their Direct Protocol and Co-operative Protocol establish a secure pair-wise communication channel between any pair of sensors in the sensor network by assigning a small set of random keys to each sensor as key seeds, executing key discovery, and setup procedure.

Besides using the probabilistic theory, some approaches [39]-[43] exploit deployment knowledge or location information to ease key management. For example, Du, et al. [40] improve the security performance of the random key pre-distribution scheme by exploiting deployment knowledge and avoiding unnecessary key assignments. Their scheme is based on the following: dividing the key pool into small key pools corresponding sensor groups; dividing the deployment area into grids; and a special key-setup making the nearby key pools share more keys. Instead of randomly distributing keys from a large key pool to each sensor, Huang, et al. [41] propose a structured key-pool random key predistribution (SK-RKP) scheme to systematically distribute secret keys to each sensor from a structured key pool. Their key predistribution scheme includes two steps: key predistribution within a given zone and key predistribution for two adjacent zones. After the deployment of sensors, each sensor first sets up pairwise keys with all neighbors within its zone; then it sets up a pairwise key with its neighbors located in adjacent zones.

- **Determinate schemes**

Contrary to probability schemes, some of approaches guarantee that any two intermediate nodes can share one or more predistribution keys. We call this type of schemes as determinate schemes, e.g. [44]-[46]. In some of theses schemes, they suppose that there is an interval secure time (during this interval, small number of shared keys is secure enough for bootstrapping process) after sensor deployment, and systems can utilize this interval time to establish security and transmit keys between neighbor nodes. Dutertre, et al. [68] also use the same idea in order to improve key management efficiency by introducing small set of shared keys in initial trust.

In [44], Chan and Perrig describe Peer Intermediaries for Key Establishment (PIKE), a class of key-establishment protocols that use one or more sensor nodes as a trusted intermediary to perform key establishment between neighbors. Unlike random key-establishment protocols, the key establishment of PIKE is not probabilistic, and any two nodes are guaranteed to be able to establish a key. The communication and memory overheads of PIKE protocols scale sub-linearly $(O(\sqrt{n}))$ with the number of nodes in the network. Though PIKE in [44] increases the security performance and solves the high density requirements in random key predistribution schemes (RKP) and some structure random key predistribution schemes (SRKP), e.g. [34], [35], [42], the deployment of PIKE requires more complex work than random deployment schemes.

Another example of deterministic security scheme, LEAP (Localized Encryption and Authentication Protocol) [45] does not expose the pairwise keys between other nodes when the network is compromised by a fraction of sensor nodes. To ease the overhead of key management, LEAP supports four types of keys for each sensor node which is appropriate for all types of communication in sensor networks – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. LEAP also supposes the interval secure time for bootstrapping process.

Sensor deployments may be static, but researchers have recently been making a case for mobile collector nodes to enhance data acquisition. Zhou, et al. in [46] analyze the impact of mobile collector compromises on the reliability of data received by the base station, and the circumstances under which reliability can be guaranteed first. Then they present mGKE (a Group-based Key Establishment scheme for mobile sensor networks), which allows any pair of neighboring sensors to establish a unique pairwise key, regardless of sensor density or distribution.

Lee and Stinson in [47] present two combinatorial design theory based deterministic schemes: the ID-based one-way function scheme (IOS) and the deterministic multiple space Blom's scheme (DMBS). They further discuss the use of combinatorial set systems in the design of deterministic key predistribution schemes for WSNs in [48]. They analyze the combinatorial properties of the set systems that relate to the connectivity and resilience of the resulting distributed sensor networks.

2) Hybrid Cryptography Schemes: Though most framework use one type of cryptograph, there still exist some schemes that use both asymmetric-key and symmetric-key cryptographs. For example, a hybrid scheme proposed by Huang, et al. in [49] balances public key cryptography computations in the base station side and symmetric key cryptography computation in sensors side in order to obtain adorable system performance and facilitate key management. On one hand, they reduce the computation intensive elliptic curve scalar multiplication of a random point at the sensor side, and use symmetric key cryptographic operations instead. On the other hand, it authenticates the two identities based on elliptic curve implicit certificates, solving the key distribution and storage problems, which are typical bottlenecks in pure symmetric-key based protocols.

3) One Way Hash Schemes: To ease key management, many approaches use the one-way key method that comes from one-way hash function technique. For example, Zachary [50] propose a group security mechanism based on one-way accumulators that utilizes a pre-deployment process, quasi-commutative property of one-way accumulators and broadcast communication to maintain the secrecy of the group membership. Another group security mechanism proposed by Dutta, et al. in [51] also use one-way function to ease group node joining or revocation. Their scheme has self-healing feature, a good property that makes the qualified users recover lost session keys over a lossy mobile network on their own from the broadcast packets and some private information, without requesting additional transmission from the group manager.

The one-way hash function can also adapt to conduct public key authentication. For example, Du, et al. [52] use all sensors' public keys to construct a forest of Merkle trees of different heights, and by optimally selecting the height of each tree, they can minimize the computation and communication costs. To ease the joining and revocation issues of membership in broadcast or group encryption, many approaches use predistribution and/or a local collaboration technique. For example, RBE (Randomized Broadcast Encryption scheme), proposed by Huang and Du in [53], uses a node-based key predistribution technique. Besides predistribution future group keys, the group rekeying scheme of Zhang and Cao [54] also adopts the neighbors' collaboration.

4) Key Infection Schemes: Contrary to most of key management using pre-loaded initial keys, Anderson, et al. [55] propose a key infection mechanism. In a key infection scheme, different from key pre-distribution schemes, no predistribution key is stored in sensor nodes. This type of schemes establishes secure link keys by broadcasting plaintext information first. This type of schemes is not secure essentially. However, Anderson, et al. show that their key infection scheme [55] is still secure enough for non- critical commodity sensor networks after identifying a more realistic attacker model that is applicable to these sensor networks. Their protocol is based on the assumption that the number of adversary devices in the network at the time of key establishment is very small (in their results, less than 3% of the devices are adversaries).

Similar to scheme in [55], Miller and Vaidya in [56] propose a predistribution scheme that allows neighboring sensors to establish secure link keys from plaintext keys that are broadcast by sensors in their neighborhood. Their scheme has better security performance than [55] by utilizing a special property of hardware - multiple channels available on some sensor hardware, and spatial diversity of device locations.

5) Key Management in Hierarchy Networks: Though many key management approaches are based on a normal flat structure, there are still some approaches [57]-[65] that utilize a hierarchical structure in order to ease the difficulties by balancing the traffic among a command node (base station), gateways, and sensors. These are the three parts of networks that have different resources.

In this type of key management, some use the physical hierarchical structure of networks such as [57]-[63], while others [64], [65] implement their hierarchy key management logically in physical flat structure sensor networks, which only include a base station and sensors. For example, LKHW (Logical Key Hierarchy for Wireless sensor networks), proposed by Pietro, et al. in [65], integrates directed diffusion and LKH (Logical Key Hierarchy) where keys are logically distributed in a tree rooted at the key distribution center (KDC). A key distribution center maintains a key tree that will be used for group key updates and distribution, and every sensor only stores its keys on its key path, i.e. the path from the leaf node up to the root. In order to efficiently achieve confidential and authentication, they apply LKHW: directed diffusion sources are treated as multicast group members, whereas the sink is treated as the KDC.

B. Summary

Key management is the linchpin of cryptograph mechanism. Most proposals use a key-predistribution technique to easy key management. Some protocols use the probabilistic theory to calculate the probability that neighbor nodes have shared keys, and others have the deterministic property so that there exists one or more shared keys between a node and its neighbors. Some protocols unite node identity in key management. Classifying different types of keys can ease key management. Integrating the localization of sensors and key predistribution can provide good security performance and minimize the effect of node compromise. Some protocols provide a threshold property while others provide gradual resilience for node compromise. Considering network structure may help designing key management, especially in hierarchy sensor networks. To decrease the number of predistribution keys stored in sensor nodes, some approaches assume that there is an interval secure time after deployment. During this interval time, predistributing a small number of keys in sensor nodes is secure enough. To ease the difficulty of key management, some approaches utilize deployment knowledge, special structure of cluster sensor networks, key classifications, one-way hash functions, etc. Some security mechanisms only use one of cryptographs while others use both public-key and symmetric-key cryptographs. After reviewing current researches, we give our recommendations of key management as follows:

- Cryptograph choosing: Symmetric cryptography is the first selection;
- Key-predistribution usage: Most symmetric schemes use key-predistribution to ease the difficulty of key management;
- Master keys usage: It may consume less computing resources and still provide enough security to store a small number of key-seeds in sensor nodes before deployment and establish security based on these seeds in short time.
- Combing location and deployment information: Integrating location information or deployment knowledge in key management schemes will ease security design and provide better security performance;
- Combing node identity: Integrating node identity in the process of key producing will make a system more secure;
- Usage of various types keys: Using different types of keys for different types of communication may ease the overhead of key management and make system more secure;
- Usage of one-way hash schemes: Using variations of one-way hash functions sometimes can ease key management design, especially for group node joining or revocation;
- Distributed structure or centralized structure: A distributed mechanism has better resilience than a centralized mechanism in large scale networks;
- Usage of special structure: Considering network structure may help designing key management, especially in hierarchy sensor networks;
- Importance of re-keying: Re-keying is very important in defending against cryptography attacks and an adaptive re-keying mechanism may be a good choice in defending against cryptography attacks;
- Using suitable schemes: Different schemes may have different advantages and shortcomings. For example, the threshold schemes have some advantages than other schemes when the number of compromised nodes is less than the threshold. However, when the number of compromised nodes is larger than the threshold, the security performance of this type of scheme will decrease largely than other schemes. Security designers should carefully analyze the application environment and adopt suitable schemes for the application.

Though there is a lot of research focused on key management, and most of them provide some extent of prevention from node compromise, the design of key management protocols is still largely open to research. Open research issues include following:

- Most key management schemes discussed in literature so far are suitable for static WSNs. Following technique advance, key management and security mechanisms for mobile WSNs should be considered and become a focus of attention.
- Most current approaches assume that the base station is trustworthy. However, there may be situations (e.g. in the battle field) where the base station is not secure as assumed. New schemes need to be designed to secure the base station.
- Though many key management approaches consider defending against node compromise, the efficiency and security performance is not high when their mechanisms are deployed in some special application environment (e.g. in the battle field). In their mechanisms, they imply the

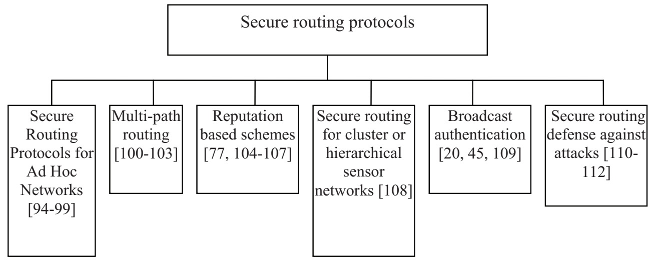
Secure routing protocols
Secure Routing Protocols for Ad Hoc Networks [94-99]
Multi-path routing [100-103]
Reputation based schemes [77, 104-107]
Secure routing for cluster or hierarchical sensor networks [108]
Broadcast authentication [20, 45, 109]
Secure routing defense against attacks [110-112]

Fig. 5. Taxonomy of secure routing.

probability of node compromise to be the same for every node. However, when their security systems are deployed in a different environment from their supposition, the security performance will decrease largely. For example, in battlefield surveillance, the probability of nodes of being compromised in an enemy controlled area is larger than in our controlled areas. Under such environment, the security performance will decrease because: the system has the same capability to defend against node compromise in all areas, while adversaries attack the system with different strengths in each area; thus making the system unable to provide enough security in some areas, while it provides more security than needed in other areas [69]. Thus, the study of node compromise distribution and integrating it in key management is a promising research area.

VI. Attack Detections and Preventions

A. *State-of-the-Art*

Security issues mainly come from attacks. If no attack occurred, there is no need for security. Detecting and defending against attacks are important tasks of security mechanisms. Attacks in WSNs are classified as external attacks and internal attacks. Compared with external attacks, internal attacks are hard to be detected and prevented. Thus, besides introducing some normal attack detecting mechanisms, we also describe some special node compromise detecting methods. Fig. 5 shows the taxonomy.

1) Attack Detecting and Prevention Mechanisms:

- **Normal external attack defenses**

Currently, there are some approaches that are focus on external attacks, described as the following:

- Sybil attack: Newsome, et al. in [15] establish taxonomy of the Sybil attacks (A Sybil attack occurs when a single node illegally claims multiple identities to other nodes in the network) by distinguishing different attack types and proposing several methods to identify these attacks, including radio resource testing, key validation for random key predistribution, position verification, and registration.
- Wormhole attack: In a wormhole attack, an adversary tunnels messages received in one part of the network over a low-latency link and replays them in a different part to make a fake that these two parts are very close. Normally, wormhole attacks need two distant colluding malicious nodes to communicate directly through relaying packets along an out-of-bound channel available only to the attackers. Hu, et al. [70] present a mechanism, packet leashes, for detecting and thus defending against wormhole attacks, and a specific efficient authentication protocol, TIK(TESLA with Instant Key disclosure), that implements leashes. A leash is any information that is added to a packet and is designed to restrict the packet's maximum allowed transmission distance. They distinguish between a geographical leash, which ensures that the recipient of the packet is within a certain distance from the sender, and a temporal leash, which ensures that the packet has an upper bound on its lifetime. The latter restricts the maximum travel distance, since the packet can travel at most at the speed of light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect whether the packet traveled further than the leash allows. Wang and Bhargava [71] propose a mechanism, MDS-VOW (Multi-Dimensional Scaling – Visualization of Wormhole), to detect wormholes by using multi-dimensional scaling to reconstruct the layout of the sensors and adopting a surface smoothing scheme to compensate the distortions caused by distance measurement errors.
- Node replication attack: It can be detected by Randomized Multicast and Line-Selected Multicast [72]. Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while Line-Selected Multicast uses the topology of the network to detect replication nodes.
- Jamming attack: Li, et al. in [73] study controllable jamming attacks in WSNs, which are easy to launch and difficult to detect and confront. They derive optimal strategies or policies for both jammer and the network defense system under two cases: perfect knowledge of the jammer and the defense system, lack of knowledge of the attacker and the network.

- **Attack/failed node detection**

As a whole, most attack detecting methods can be classified as centralized approaches or neighbors' cooperative approaches.

- Centralized approaches: The type of method uses the base station to detect attacks. Although the schemes in [74], [75] are mainly used to diagnose failed nodes, the idea can also be adapted to detect attacks. In the approach of [74], sensor networks are diagnosed by injecting queries and collecting responses. To reduce the large communication overhead, which results in failure detection latency, their solution reduces the response implosion by sacrificing some accuracy. Staddon, et al. in [75] propose another centralized approach to trace the failed nodes. Nodes append a little bit of information about their neighbors to each of their measurements and transmit them to the base station to let the latter know the network topology. Once the base station knows the network topology, the failed nodes can be efficiently traced using a simple divide&conquer strategy based on adaptively routing update messages.
- Neighbors' cooperative approach: In neighbors' cooper-

ative approach, neighbor nodes of a given node collect neighbors' information and make a collective decision to detect attacks. Wang, et al. in [76] propose a distributed cooperative failure detecting mechanism to let the neighbors of a faulty node cooperate to detect the failure. To achieve neighbors' communication efficiency, they propose Tree-based Propagation-Collection (TPC) protocols to collect the information from all neighbors of the suspect with low delay, low message complexity, and low energy consumption. Watchdog [77] also uses neighbors to identify misbehaving nodes. Ding, et al. in [78] propose another localized approach to detect the faulty sensors by using neighbors' data and processing them with the statistical method. Threshold approaches is a special type of neighbors' cooperative approach, e.g. [7], [80]. Recently, Liu, et al. in [81] introduce a new neighbors' cooperative approach to detect insider attacks. The nice feature of their algorithm is that it requires no prior knowledge about normal or malicious sensors, which is important considering the dynamic attacking behaviors. Further, their algorithm can be employed to inspect any aspects of networking activities, with the multiple attributes evaluated simultaneously, which is better than the previous schemes, e.g. [82].

- **Denial of service attack and countermeasures**

Denial of service (DoS) means that the adversaries attempt disrupting, subverting, or destroying sensor networks in order to diminish or eliminate its capacity to perform its expected function. DoS can disrupt sensor nodes, communications among nodes, and the base station to implement their goal, which is disabling sensor network availability. Draining the battery by repeating service request attacks, benign repeating energy-hungry tasks, or repeating malignant burden tasks is also a special type of DoS [92]. Denial-of-Message attack [93] is another type of DoS in which adversaries deprive other nodes from receiving broadcast messages. To prevent DoS attacks, we can adopt the following methods:

- Watchdog and Reputation Rating based scheme: Marti, et al. in [77] propose a watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. The Watchdog Scheme is further investigated and extended to Reputation Rating Scheme [82]-[84]. In the Reputation Rating Scheme the neighbors of any single node collectively rate the node according to how well the node executes the functions requested of it. Compared to malicious nodes disrupting the network, selfish nodes only refuse to perform any function requested by the others, such as packet forwarding, to save energy. Reputation Rating Scheme conquers the selfish nodes by giving them a bad strike.
- Virtual currency: Virtual currency systems [85]-[87] use credit or micro payments to compensate for the service of a node. A node receives a virtual payment for forwarding the message of another node, and this payment is deducted from the sender (or the destination node). Two examples of such systems are: Nuglets [85], [86] and Sprite [87]. Nuglets has two models: Packet Purse Model and Packet Trade Model. In the Packet Purse Model, each packet is loaded with enough Nuglets by the source, and each forwarding host takes out some Nuglets for its forwarding service. The advantage of this approach is that it discourages users from flooding the network. In the Packet Trade Model, packets are traded for Nuglets by the intermediate nodes. Each intermediate node buys the packet from the previous node with some Nuglets, and sells it to the next node for more Nuglets, and the destination has to pay the total cost of forwarding the packet. The direct advantage of this method is that the source does not need to know how many Nuglets need to be loaded into the packet. To prevent illegal manipulation of the nodes' Nuglets, tamper-proof hardware is required at each node to store all the relevant IDs, Nuglets counter, and cryptographic materials. Sprite [87], a simple, cheat-proof, credit-based system uses credit to provide incentives for mobile nodes to cooperate and report actions honestly. The basic idea of this scheme is as follows: a system has a Credit Clearance Service (CCS) to determine the charge and credit to each node involved in the transmission of a message. Payments and charges are determined from a game theory perspective. In this scheme, the sender is charged to prevent a denial-of-service attack to the destination by sending it a lot of traffic. A node receives credit only when the next node on the path reports a valid receipt to the CCS to acknowledge the successful transmission.

2) Special Node Compromise Detecting Mechanisms: Although many node compromise detecting mechanisms use centralized detecting methods or neighbors' cooperative/localized methods to monitor the activities of nodes, there are still some mechanisms use code testing methods and a special scheme uses location verification method.

- **Code testing schemes**

In the context of node compromise code testing schemes in WSNs, some implement their schemes by software-based, while others use hardware to assist their mechanisms.

- Software-based approach: In software-based approaches, such as [88], [89], rely on optimal program code and exact time measurements. These approaches enable software-based attestation by introducing an optimal program verification process that verifies the memory of a sensor node by calculating hash values of randomly selected memory regions.
- Hardware-based approach: Normal hardware-based approaches such as [90] are based on public-key cryptography and require extensive computational power, as well as the transmission of large messages, making these approaches not usable in WSNs. Krauss, et al. [91] suppose that some cluster nodes posses much more resources than the majority of clusters and are equipped with a Trusted Platform Module in the hybrid WSNs. Their hardware-based attestation protocols use the nodes equipped with Trusted Platform Module as trust anchors and can enable attestation with more efficiently. However, their mechanisms can only make sense in Hybrid WSNs.

- **Location verification schemes**

Song, et al. in [14] provide a method to detect node compromise by comparing the previous position of nodes with current position. The main idea of their mechanism is based on the assumption that a node compromise often consists of three stages: physically obtaining and compromising the sensors, redeploying the compromised sensors, and compromised nodes launching attacks after their rejoining the network. In some applications an attacker may not be able to precisely deploy the compromised sensors back into their original positions. Their mechanism can detect compromise events when compromised nodes change positions or identities. But sometimes adversaries can compromise the nodes by communicating them, breaching their security mechanism, and controlling them without physically touching them or moving their positions. Under such condition, their mechanism will not detect the compromise events.

B. Summary

Normally, most attack detecting mechanisms belong to centralized approaches or neighbors' cooperative approaches. Centralized approaches gather the data from the monitoring node and compare them with the data from its neighbor nodes. Based on the comparing result, the system makes a decision whether the given node is attacked or not. The disadvantage of this method is that it introduces more routing traffic from the given node to the base station. While in neighbors' cooperative approaches, neighbor nodes of the given node make a collective decision to detect attacks. Though it does not need transfer larger data to the base station, it introduces more computing process and monitoring tasks for neighbor nodes. In all, Watchdog and Reputation Rating based or Virtual currency methods are able to prevent DoS attacks in some extent. Code testing methods and location verification methods open our eyes to node compromise detection, though they need more work to improve. For example, code testing mechanisms introduce more communication overheads between sensor nodes and the base station.

Though there is a lot of research focused on attack detection and prevention, and most of them provide some good results, there is still much work need to be studied in the future. Open research issues include following:

- Currently, most current detecting systems monitor all the nodes in the system without emphasis, and the system should decentralize their resources evenly in all nodes in order to monitor whether they have larger compromise probabilities or not. That makes the detecting mechanism less efficient. Due to the heavy work, the system performance may decrease largely, and may even make this work unpractical. A good ideal is that the system chooses those nodes that have larger probability to be attacked as the main monitoring object. However [69] only provides the idea. How to implement this idea still need more work.
- Although above code testing schemes introduced in section 6.1.2 can detect whether the given node is compromised or not, the assumptions of these schemes are very strong. For example, the scheme in [89] assumes that the attacker's hardware devices were not present in the sensor network for the duration of the repair process. Most of time, attackers use big nodes, such as laptops, as the attacking devices, and these attacker nodes present and attack the sensor network all the time. Furthermore, all these approaches do not tell us when these mechanisms are executing. They just say that the mechanisms are executing by the request of the base station. So their systems must have some other mechanisms to invoke these code testing schemes. However they do not provide any invoking mechanisms in their research work. The algorithm of the invoking mechanisms is very important because: if the checking interval for each node is small, these code testing schemes introduce a lot of communication cost and consume large computing resources for the sensor node; on the contrary, if the checking interval for each node is large, the compromised nodes may have long time to paralyze the network. An invoking algorithm that makes code testing mechanisms more efficient and effective needs to be investigated.
- Most proposed attack detecting mechanisms focus on static WSNs, ignoring mobility. Attack detecting schemes for mobile WSNs are desirable.

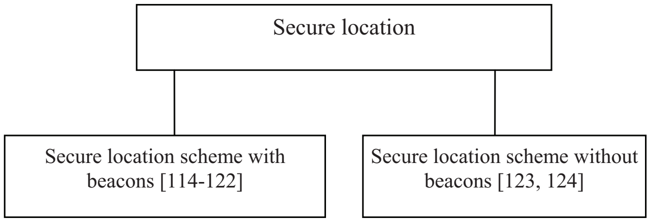
Secure location
Secure location scheme with beacons [114-122]
Secure location scheme without beacons [123, 124]

Fig. 6. Taxonomy of secure location schemes.

VII. SECURE ROUTING

A. State-of-the-Art

WSNs use multi-hop routing and wireless communication to transfer data, thus incur more routing attacks. There are a lot of approaches to ease routing security. In this section, we review existing secure routing approaches. Fig. 6 shows the taxonomy of secure routing.

1) Secure Routing Protocols for Ad Hoc Networks: Because WSNs came from ad hoc, some of secure routing algorithms [94]-[99] in the latter are still valued to be reviewed though they may have difficulty to be suited to sensor networks. Some secure AODV algorithms [94], [95] that may be adapted in WSNs have some effects on defending against external attacks because they suggest secure routing information. These security mechanisms still meet security issues when the nodes are compromised and the security information such as key is disclosed to the attackers.

A certificate approach, URSA, a ubiquitous and robust access control solution proposed by Luo, et al. in [96], uses the multiple nodes decision to certify/revoke a ticket to ensure access control service ubiquity and resilience. Sanzgiri, et al. in [97] also propose a secure routing protocol based on certificate. Their protocol, Authenticated Routing for Ad hoc

Networks (ARAN), works to defend against identified attacks under such a scenario where no network infrastructure is pre-deployed, but a small amount of prior security coordination is expected before deployment.

Papadimitratos and Haas [98] propose a route discovery protocol that it only requires the security association between the node initiating the query and the sought destination only in order to defend against routing attacks, such as fabricated, compromised, or replayed attacks for mobile Ad Hoc Networks. An on-demand routing protocol for ad hoc to provide resilience to Byzantine failures (which include nodes that drop, modify, or mis-route packets in an attempt to disrupt the routing service), proposed by Awerbuch, et al. in [99], can be separated into three successive phases: route discovery with fault avoidance by using flooding and cryptographic primitives, Byzantine fault detection by using adaptive probing technique to identify a malicious link after log n (n is the length of the path) faults occurred, and link weight management by multiplicatively increasing the malicious link weight. Their protocol avoids malicious links in the routing paths because the system uses an on-demand route discovery protocol that finds a least weight path to the destination.

2) Multi-Path Routing: Some approaches use multi-path routing and neighbor collaboration techniques, such as [100], [101]. Multi-path routing, location disguise, and relocation methods can be used to protect base stations [101]-[103]. In the environment where the network only has a small number of compromised nodes, Multi-path schemes provide more reliable routing, though they introduce more communication overheads. However, in the environment where the network has a large number of compromised nodes, if the compromised can modify the routing data, system may involve more security issues.

3) Reputation Based Schemes: Reputation based schemes normally need neighbor nodes corporation to control the credit, reputation, etc. Routing paths will path the nodes with good reputation. In ad hoc networks, Watchdog and Pathrater [77] can be regarded as one of the earliest works in trust-based routing schemes. A probabilistic routing algorithm, ARRIVE, is proposed by Karlof, et al. in [104] to defend link failures, patterned node failures, and malicious or misbehaving nodes without resorting to periodic flooding of the network. The main idea of their algorithm is that: the next hop in the routing path is chosen probabilistically based on link reliability and node reputation; it uses multiple paths, and it ensures that the packets of the same event use different outgoing links when they meet at one node.

SIGF (Secure Implicit Geographic Forwarding) [105] also needs neighbor collaboration to choose the nodes in the routing path. FBSR [106], a feedback based secure routing protocols gets feedback from both the nearby neighbors and the base stations. Feedback serves as the dynamic information of the current network, with which sensor nodes make forwarding decisions in a secure and energy aware manner. These proposals collect neighbor feedbacks or information to decide routing paths. They are based on reputation or corporate decision, etc., and they can prevent routing paths from passing some nodes that have less reliability factors or the reputations are bad. Besides considering security, the trust-based routing scheme proposed by Hung, et al. in [107] also takes into account the metric of network lifetime.

4) Secure Routing for Cluster or Hierarchical Sensor Networks: Some researchers utilize the special structure in physical or logical cluster or hierarchical sensor networks in order to provide more efficient secure routing algorithms. For example, Tubaishat, et al. in [108] propose an energy efficient level-based hierarchical system. In their approach, they divide the sensor nodes into different levels. The lower-level sensor nodes only sense and disseminate data, whereas the higher-level sensors find the shortest path to the sink node and aggregate data in addition to forwarding it. A sensor becomes a cluster head and is valued as level 2 if it has the highest number of neighbors (NBR). Sensors are initiated at level 0 when embedded in the network. The incremental level depends on a sensor's reliability and its energy consumption. When a sensor finds its neighbors it upgrades itself to level 1 and then to level 2 if it becomes a cluster head. A sensor connected to two or more cluster heads upgrades itself to level 3 (they call this node the root). Based on the level classifications, they propose a new routing protocol algorithm that depends on the number of neighbors and their levels to disseminate the queries and data. The level-based hierarchical routing protocol compromises between shortest path and energy consumption. Based on the usage of hierarchical structure of sensor networks and symmetric key, they propose a secure routing protocol. In addition, they propose a group key management scheme which every sensor node contributes its partial key for computing the group key.

5) Broadcast Authentication: μTESLA proposed by Perrig, et al. in [20] is an authenticated broadcast protocol for the SPINS. It divides time into intervals of equal duration and assigns each time slot a corresponding key. μTESLA introduces asymmetry through a delayed disclosure of symmetric keys resulting in an efficient broadcast authentication scheme. Each MAC key is a key from the one-way key chain, generated by a public one-way function F. The base station chooses the last key K_n from the chain, and repeatedly applies F to compute all other keys: $K_i = F(K_{i+1})$. The base station sends packets with MAC. The receiver node stores the packet in a buffer. At the time of key disclosure, the base station broadcasts the verification key to all receivers. During that time, the receiver can use the disclosure key to authenticate the packet stored in its buffer. If a node wants to broadcast information, it must send the information to the base station first and then the base station broadcasts the information. All of operations in SPINS need the network to keep time synchronization between nodes, thus the base station makes the latter susceptible to attack and has more traffic nearer the base station.

Liu and Ning in [109] go a step to present a multi-level key chain scheme to improve μTESLA key distribution efficiency by using pre-determination and broadcast to remove its requirement of a unicast-based distribution of initial key chain commitments to save communication overhead in large distributed sensor networks.

μTESLA and its extension provide broadcast authentication for base station, but they are not suitable for local broadcast authentication because: they cannot provide immediate authentication; the communication overhead is high between sensors and the base station; packet buffering requires more storage space for sensors. Zhu, et al. in [45] propose a one-way key chain for one-hop broadcast authentication based on pairwise key to solve the issues in μTESLA.

6) Secure Routing Defense Against Attacks: PRSA (path redundancy based security algorithm) [110] uses alternative routing paths for each data transmission call to overcome the sensor network attack. To enhance network reliability, PRSA allows sensor node data to be sent on defined routing paths using various transmission modes including round robin, redundant and selective modes.

To defend against node compromise, An, et al. in [111] present a route recovery scheme called Route Recovery by One-Hop Broadcast (RROB) that removes compromised nodes from the current route and reconstructs the route without depending on central mediation. RROB reconstructs the new path based on the current path and bypass the compromised nodes in the current path. Instead of flooding packets in the network, RROB utilizes the neighbors of the compromised nodes to bypass the compromised nodes to decrease the communication overhead and the energy consumption.

To prevent packet-tracing attack, in which an adversary traces the location of a receiver by eavesdropping and following the packets transmitted in the sensor network, Jian, et al. in [112] propose a location privacy routing protocol (LPR) that is easy to implement and provides path diversity. Combining with fake packet injection, LPR is able to minimize the traffic direction information that an adversary can retrieve from eavesdropping. By making the directions of both incoming and outgoing traffic at a sensor node uniformly distributed, the new defense system makes it very hard for an adversary to perform analysis on locally gathered information and infer the direction to which the receiver locates.

B. Summary

Currently, there are a lot of secure routing algorithms for WSNs. Many routing algorithms are reputation based schemes, which rely on neighbor nodes' corporation. Some approaches utilize the special structure (cluster WSNs) to balance the computing and transmission overheads between big nodes and normal nodes. Some researchers study some types of attacks, and propose special algorithms to prevent the specified attacks. Others use cache to improve the efficient [113].To provide routing reliability, some adopt multi-path techniques. One-way functions are the normal method to provide broadcast authentication. Though a lot of protocols are proposed to secure routing, the design of new algorithms is still largely open to research. Open research issues include following:

- Most current proposals are suitable for static WSNs. Designing secure routing algorithms for mobile WSNs is complex and current secure routing algorithms will meet issues when they are applied in mobile environments. For example, reputation based schemes will meet difficulties when they adapt to mobile environments.
- Undetected node compromise issues: The current cryptography mechanisms, such as authentication, identification, etc. may detect and defend against node compromise in some extent. However, most compromise activities cannot be detected immediately because any detecting mechanism needs time to collect and process collected data, and the fraudulent action of adversaries (adversaries don't want system to notice their attacking activities.) even makes the detecting time longer. In such condition, there exist some intervals when some nodes are compromised nodes but the system has not detected them. During these intervals, routing paths in current algorithms, such as [111], may pass the undetected compromised nodes, the nodes that have already been compromised but the system has not detected them. Thus, current approach cannot conquer undetected node compromise. Designing secure routing that can defend against undetected node compromise is a promising research area [69].
- Currently most proposals only consider security metrics and only a few of them evaluate other metrics, e.g. [107]. More metrics, such as QoS (quality of service) need to be considered in addition of security.
- Though some secure routing algorithms are proposed based on hierarchical sensor networks, most of these studies did not show the different effects such as energy consummations, security, etc. due to different cluster size. What's more, though these algorithms may ease secure routing issues, they bring complex cluster management issues and costs. More elaborate studies need to be done in the future.
- Routing maintenance: During the lifetime of a sensor network, the network topology changes frequently, and routing error messages are normally produced. Preventing unauthorized nodes from being producing this type of message is important and needs more studies.

VIII. Secure Location

A. State-of-the-Art

Location information is very important in some applications of sensor network, such as reconnaissance of opposing forces. Many monitoring applications require near accurate position besides event self. Besides this type of application, many routing protocols or other security mechanisms also need location information or distance information among neighbor nodes. Thus, providing secure and reliable location information in some special applications under adversaries' attacks need pay more attention. Fig. 7 shows the taxonomy of secure location schemes.

1) Secure Location Scheme With Beacons: In some location systems, some sensors have a position system such as GPS to locate their positions. We call this type of sensors beacon nodes. These location systems use location information from these beacon nodes and some positioning and ranging techniques to construct the whole location systems. Positioning and ranging techniques in wireless networks mainly rely on measurements of the times of flight of radio or ultrasound signals, and on the measurements of received strengths of radio signals of devices. However, these methods are highly vulnerable to attacks from dishonest nodes and external attackers.

A mechanism for position verification, called Verifiable Multilateration (VM), proposed by Capkun and Hubaux in

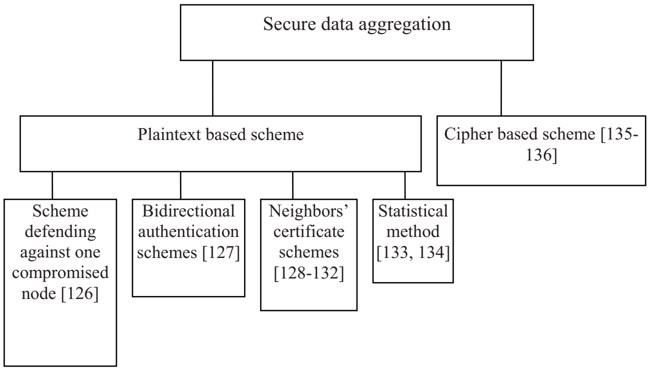
Secure data aggregation
Plaintext based scheme
Cipher based scheme [135-136]
Scheme defending against one compromised node [126]
Bidirectional authentication schemes [127]
Neighbors' certificate schemes [128-132]
Statistical method [133, 134]

Fig. 7. Taxonomy of secure data aggregation schemes.

[114], is based on Distance bounding techniques [125] that can prevent compromised nodes from reducing the measured distance. VM use the distance bound measurements from three or more reference points (verifiers) to verify the position of the claimant.

Lazos and Poovendran in [115] propose a range overlapping method instead of using the expensive distance estimation method. Its main idea is as follows: each locator transmits different beacons with individual coordinates and coverage sector areas. After receiving enough sector information from different locators, the sensor estimates its location as the center of gravity of the overlapping region of the sectors that include it. Instead of solving the secure location determination problem, Sastry, et al. in [116] introduce the in-region verification problem (a problem how verifiers verify whether a prover is in a given region of interest) and show how it can be used for location-based access control.

Li, et al. in [117] propose robust statistical methods in order to make two broad classes of localization including triangulation and RF-based fingerprinting attack-tolerant. For triangulation-based localization, their adaptive algorithm uses least squares (LS) position estimator in normal status, and switches to use least median squares (LMS) instead of least squares (LS) for achieving robustness when being attacked. For fingerprinting-based location estimation, they introduce robustness by using a median-based distance metric instead of traditional Euclidean distance metrics.

Capkun, et al. in [118] analyze the attack model in two types of positioning systems: node-centric and infrastructure-centric. In a node-centric positioning system, a node computes its position by observing signals received from public base stations with known locations. Infrastructure-centric positioning systems are those in which the infrastructure computes positions of nodes based on their mutual communication. After the analysis of attack models, they propose a new approach to secure localization based on hidden and mobile base stations. Their approach enables secure positioning with a broad spectrum of positioning techniques: ultrasonic or RF, based on received signal strength or on time of signal flight. Their secure position system need more base stations while most WSNs only have one base station. Furthermore, most verification work is executed by base stations, thus incurring more communication overheads.

Different from many proposals defending against cryptographic attacks, Chen, et al. in [119] analyze the problem of detecting non-cryptographic attacks on wireless localization, such as signal attenuation and amplification, that cannot be addressed by traditional security services. In Multilateration localization approaches, they build a mathematical model and derive an analytic solution for attack detection using the residuals of an LLS (Linear Least Squares) regression for easy conducting. In signal strength based approaches, they use the minimum distance between an observation and the database of signal strength vectors as the test statistic to perform attack detection.

Hwang, et al. in [120] propose a secure localization mechanism that detects phantom nodes, which claim fake locations, without relying on any trusted entities, an approach different from the other approaches. Their algorithm includes two main phases: distance measurement phase and filtering phase. In the first phase, each node measures the distances to its neighbors. In the second phase, each node projects its neighboring nodes to a virtual local plane to determine the largest consistent subset of nodes. After the completion of the two phases, each node establishes a local view without phantom nodes.

Beacon location systems will meet difficulty issues when the beacon nodes are compromised. To detect malicious beacon nodes, the scheme in [121] uses redundant beacon nodes instead of normal nodes in the sensing field to verify them. To defend against malicious beacon node compromise, Liu, et al. in [122] propose two methods: attack-resistant Minimum Mean Square Estimation, and collective "votes." The main idea of the first method is that the malicious location references introduced by attacks are usually inconsistent with the good ones due to their misleading characteristic. The main idea of the second technique is as follows: the deployment area is quantized as small cells; each location reference (beacon node) "votes" which cell the node belongs to; and finally the center of the selected cell is thought of as the location of the node.

2) Secure Location Scheme Without Beacons: In practical environments, sensor networks may not have beacon nodes. Under such conditions, some approaches [123], [124] estimate location by combining deployment knowledge and probability theory. Fang, et al. in [123] propose a Beacon-Less Location Discovery Scheme. Their scheme supposes that: sensors in the same group are deployed together at the same deployment point; and the locations of sensors from the same group follow a probability distribution that can be known a priori. With their supposition, they can estimate the actual location of a sensor in static sensor networks by observing the group memberships of its neighbors and using the Maximum Likelihood Estimation method. Furthermore, they propose a general scheme called Localization Anomaly Detection (LAD) [124], to detect localization anomalies that are caused by adversaries by comparing the inconsistency of location between pre-deployment and after deployment.

B. Summary

Providing reliable and accurate location is the key factor in some sensor networks when position or location information is

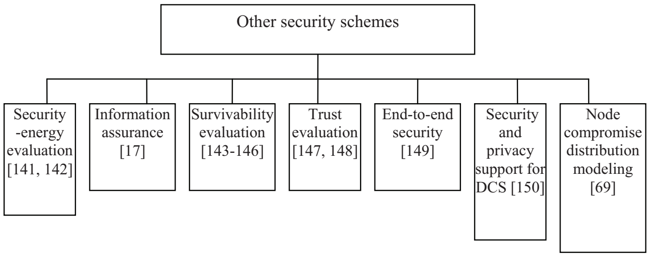
Other security schemes
Security -energy evaluation [141, 142]
Information assurance [17]
Survivability evaluation [143-146]
Trust evaluation [147, 148]
End-to-end security [149]
Security and privacy support for DCS [150]
Node compromise distribution modeling [69]

Fig. 8. Taxonomy of other security mechanisms.

the object of these networks, or if they need position information in those systems. From above review, we know that two main methods, including beacon detection and deployment estimation, can be used to locate sensors. When the first method is used, we can use multiple beacons to detect location, tolerating attacks and even malicious beacon attacks by using a voting mechanism or by utilizing statistical methods. To defend against attacks in the second location method, we only need to ensure the group membership is guaranteed by a secure mechanism. However, the second location method cannot provide accurate location information as the first method does. Currently, most of current proposals are suitable for static WSNs. Secure location algorithms for mobile WSNs in different environments need to be investigated.

IX. Secure Data Aggregation

A. State-of-the-Art

In typical data aggregation or data fusion application scenarios, the sensor nodes are spread randomly over the terrain under scrutiny and collect sensor data. Each node processes the data and coordinates with nearby nodes in order to combine their information (the process is called data fusion). The aggregate data is then forwarded to specialized gateway nodes or base stations.

Though data aggregation can reduce communication overhead significantly, it brings more security issues. In a WSN, there are usually certain nodes, called aggregators, helping to aggregate information requested by queries. In general, there are two types of attacks for data aggregation operation. The first one is that aggregators received false data from sensor nodes. This false data may be produced by the original sensor nodes or the intermediate nodes between original sensor nodes and aggregators. The second one is that the base station receives false data from compromised aggregator nodes. Of course, routing between aggregators and the base station may also meet security issues. However these issues belong to the research area of secure routing.

There are two types of secure data aggregation ways: plaintext based scheme and cipher based scheme. The intermediate nodes in the path know the content of the transferred data in the first type of scheme. In the second type of scheme, data aggregation is based on the concealed data. Fig. 8 shows the taxonomy of secure data aggregation.

1) Plaintext Based Scheme:

- **Scheme defending against one compromised node**

A secure aggregation mechanism based on delayed aggregation and delayed authentication (one way delay authentication - μTESLA [20]) instead of aggregating messages at the immediate next hop, proposed by Hu and Evans in [126] provides resilience to both intruder devices and single device key compromises. However, the mechanism may be vulnerable if a parent and a child node in the hierarchy are compromised.

- **Bidirectional authentication schemes**

Deng, et al in [127] introduce a secure in-network routing algorithms involved processes of downstream and upstream between aggregators and sensors. In the downstream stage, sensor nodes authenticate commands disseminated from parent aggregators and this is accomplished by two techniques: one-way hash chains and μTESLA. In the upstream, aggregators authenticate data produced by sensors before aggregating that data. The upstream stage requires that pairwise keys be established between aggregators and their sensor nodes.

- **Neighbors' certificate schemes**

In this type of approach [128]-[132], the aggregation report must be verified or endorsed by the neighbor nodes of the aggregator before sending out. Du, et al. in [128] propose a Witness-Based approach to assure the validation of the data sent from data fusion nodes to the base station. In their approach, some nodes around the data fusion node are selected as witnesses to monitor the data fusion results. Before the fusion data is transmitted to the base station, the system adds the witness information to them, and the base station processes the witness information and uses a voting strategy to decide whether to accept a fusion result or not.

To filter injected false data between sensors and the base station, Zhu, et al. in [130] propose an interleaved hop-by-hop authentication (IHA) scheme in which at least $t + 1$ sensor nodes have to endorse a report before it is sent to the base station, where t is the node compromise threshold. In the process of data transmission to the base station, the injected false data packets can be detected and filtered by either at or en-route to the base station. Furthermore, their scheme gives an upper bound for the number of hops that a false data packet could be forwarded before it is detected and dropped, given that there are up to t colluding compromised nodes. This scheme is particularly useful for large-scale sensor networks where a sensor report needs to be relayed over several hops before it reaches the base station and for applications where the information contained in the sensor reports is not amenable to the statistical techniques used by SIA [129] (e.g., non-numeric data). Vogt in [131] explores several message authentication methods including end-to-end, hop-to-hop, physical and virtual multipath authentication. Based on the exploration, a virtual multipath authentication method, called Canvas scheme, is introduced. In the scheme, each node will create two MACs for the next two nodes that it makes a message being authenticated twice before it is forwarded. Similar to [130], the scheme in [131] also uses interleaved authentication method with t equal to 1. That means that this scheme can detect and filter false packets under one node compromise.

Yu and Guan in [132] propose a dynamic en-route filtering scheme for false data injection attacks in wireless sensor networks. In their scheme, a legitimate report is endorsed by multiple sensing nodes using their own authentication keys generated from one-way hash chains. Cluster head uses Hill Climbing approach to disseminate the authentication keys of sensing nodes to the forwarding nodes along multiple paths toward the base station. Hill Climbing guarantees that the forwarding nodes closer to a cluster hold more authentication keys for the cluster than those nodes farther from it do, hence, the number of keys held by each forwarding node can be balanced. In filtering phase, each forwarding node validates the authenticity of the reports and drops those false ones.

- **Statistical method**

Instead of collective endorsement, some approaches use a statistical method to secure aggregation. For example, Ye, et al. in [133] propose a statistical en-route filtering (SEF) mechanism to detect and drop false reports during the forwarding process. Their mechanism attaches corporate endorsements (keyed message authentication code, MAC) in the data packet. In the process of data transmission to the base station, each node along the path verifies the correctness of the MAC's probabilistically and drops those with invalid MACs. Another approach in [134] also applies a robust statistics estimation model with noisy and error-prone data to the problem of securing aggregation in the presence of malicious or spoofed data.

9.1.2 Cipher based scheme

Different from plaintext based schemes, the intermediate nodes in the path do not know the content of the transferred data. To prevent the disclosure of data in intermediate nodes, Concealed Data Aggregation (CDA), proposed by Girao, et al. in [135], conceals sensed data end-to-end and still provides efficient in-network data aggregation without any operation of plaintext data in intermediate nodes. Their work is based on a privacy homomorphism (PH), proposed by Domingo-Ferrer in [137], a particular encryption transformation. PH allows direct computation on encrypted data. Let Q and R denote two rings, $+$ denote addition and $\times$ denote multiplication on both. Let K be the key space. They denote an encryption transformation $E : K \times\ Q \rightarrow R$ and the corresponding decryption transformation $D : K \times\ R \rightarrow Q$. Given a, $b \in Q$ and $k \in K$ they term $a + b = D_k(E_k(a) + E_k(b))$ *additively* homomorphic and $a \times\ b = D_k(E_k(a) \times\ E_k(b))$ multiplicatively homomorphic. The concept of PH is first described by Rivest, et al. in [138]. In [137] Domingo-Ferrer presents an additive and multiplicative PH which is a symmetric scheme and secure against chosen ciphertext attacks. Although Wagner in [139] shows that the proposed PH in [137] is unsecure against chosen plaintext attacks for some parameter settings, Girao, et al. in [135] argue that for the WSN data aggregation scenario, the security level is still adequate and the proposed PH in [137] can be employed for encryption transformation. CDA is suitable for aggregation functions: average and movement detection. To calculate average, an aggregator needs to know the number of sensor nodes.

Recently, Peter, et al. in [136] describe and evaluate three algorithms: Domingo-Ferrer (DFPH) [137], CMT (they denote it corresponding to the authors initials) - a Key stream based PH [140], Elliptic Curve ElGamal, that were reported to suit to the WSN scenario. The elliptic curve ElGamal (ECEG) based PH is an asymmetric cryptographic approach. As the name suggests the ECEG PH is based on the well investigated ECEG cryptographic algorithm. After careful evaluation, they discovered that none of the described algorithms provides all the desirable security goals. Despite this, it turned out that the key stream based CMT approach is the most promising one. To cope with the problems they propose two approaches. The first approach combines two algorithms so that weaknesses of one algorithm are covered by the strengths of the other one. For the second approach they face specific weaknesses and engineer mechanisms that solve the particular issues. With the considered homomorphic message authentication code and a discussion of the id-issue, they exemplary evaluate the two biggest issues of the very promising CMT algorithm.

B. Summary

Data aggregation is a normal operation to save energy and provide accurate phenomenon observation in sensor networks. Though data aggregation can reduce communication overhead significantly, it brings more security issues. In all, there are two types of secure data aggregation ways: plaintext based scheme and cipher based scheme. Compared with the second type of scheme, the first type of scheme introduces more operations of encryption and decryption, thus incurring more energy consumption. However, the latter one usually lowers the security level. In the first type of scheme, many proposals use neighbor nodes' collective endorsement or similar methods to verify the correction of the aggregation reports. Others adopt statistical methods to filter the fake data. Though a lot of protocols are proposed to secure aggregation, the design of secure routing algorithms is still largely open to research. Data aggregation is essential for WSNs and its security still needs more considerations. Open research issues include the following:

- Currently, most studies assume aggregators as big nodes. It is desirable to design a secure data aggregation scheme in the environments without big nodes.
- Since data aggregation can save system energy and introduces security issues, is it possible to design a scheme based on the different security and energy requirement?
- Though there exists one evaluation paper for CDA algorithms, new evaluation studies are still needed especially for plaintext based schemes. The evaluation metrics may include security, communication overheads, process overheads, energy consumption, etc.
- Most of current schemes are only suitable for static WSNs. Designing new secure data aggregation schemes for mobile WSNs including mobile aggregators or normal nodes still needs further studies.

X. Other Security Issues

A. State-of-the-Art

Other security issues include security-energy assessment, data assurance, survivability, etc. It's very important to study these areas due to a sensor network's special character, such as battery limitation, high failure probability nodes, easier compromised nodes, unreliable transmission media, etc. Fig. 9 shows the taxonomy of other security mechanisms.

1) Security-Energy Evaluation: As to our knowledge, few research works have been done in this area. To evaluate the relation between energy and security, Law, et al. in [141], [142] describe an assessment framework based on a system profile after carefully reviewing the dominant issues of energy-security trade-off in the network protocol and key management design space.

2) Information Assurance: Due to resource limitations of a sensor network, the transmission all of information with the same reliability requires more resources and is impractical. For the user, different types of events have different levels of importance. Based on this assumption, Deb, et al. in [17] propose an assurance level mechanism to transmit the information of different criticality with different reliability (probability to sink) using hop-by-hop broadcast.

3) Survivability Evaluation: As so far, many schemes are proposed to secure WSNs, it is crucial to build a model to evaluate these schemes with regard to survivability of a WSN. In [143], Li, et al. propose a quantitative evaluation model for a typical pre-distribution key management scheme. Their survivability evaluation model includes three major attributes: resilience, resistance, and robustness. Based on their model, they show that that increasing the key space and decreasing the multiple key space would improve the survivability of WSNs. Kim, et al. in [144] propose a survivability model with software rejuvenation methodology, which is applicable in security field and also less expensive. Based on their model, they analyze each cluster of a hierarchical cluster based WSN as a stochastic process based on semi-Markov Process (SMP) and Discrete-Time Markov Chain (DTMC). Different from other approaches considering node survivability, Kumar, et al. in [145] simulate a DDoS attack on a WSN-gateway (Most approaches denote it as the base station) of a WSN to highlight how the computing resource of the gateway can be exhausted which directly hampers or disables the data collection efforts. Skelton, et al. in [146] survey the issues and concerns surrounding the deployment and maintenance of WSNs. Their research focuses on several distinct areas affecting survivability: 1) power, 2) network/node destruction and repair, and 3) network security. They summarize that the two distinct categories of survivability: information access and end-to-end communication, are applied to all of the networking layers. Based these two requirement categories, they examine the cause of WSN failure, both hardware and software based, and then identify means by which survivability may be supported.

4) Trust Evaluation: Sun, et al. in [147] presents a framework for trust evaluation in distributed networks. They address the concept of trust in computer networks, develop trust metrics with clear physical meanings, develop fundamental axioms of the mathematical properties of trust, and build trust models that govern trust propagation through third parties. Further, they identify some attacks that can reduce the effectiveness of trust evaluation, and develop some techniques to defend against these attacks. Then, they design a systemic trust management system. Their framework can be used to assist route selection and malicious node detection. Crosby, et al. in [148] describes a reputation based trust framework with a mechanism for the election of trustworthy cluster heads in cluster based WSNs. Their cluster formation algorithm establishes trusted clusters by the help of pre-distributed keys.

5) End-to-End Security: Most existing security designs provide a hop-by-hop security paradigm only, which leaves the end-to-end data security at high stake. To provide end-to-end data security, Ren, et al. in [149] propose LEDS: a location-aware end-to-end security framework, in which each node only stores a few secret keys and those secret keys are bound to the node's geographic location. In LEDS, the targeted terrain is virtually divided into multiple cells using a concept called virtual geographic grid. LEDS then efficiently binds the location (cell) information of each sensor into all types of symmetric secret keys owned by that node. By this means, the impact of compromised nodes can be effectively confined to their vicinity. In LEDS, each node computes three different types of location-aware keys: 1) two unique secret keys shared between the node and the sink and used to provide node-to-sink authentication; 2) a cell key shared with other nodes in the same cell that is used to provide data confidentiality; and 3) a set of authentication keys used to provide cell-to-cell authentication and en-route bogus data filtering. LEDS ensures both node-to-sink and node-to-node authentication along report forwarding routes. Moreover, LEDS guarantees efficient en-route bogus data filtering, and is highly robust against DoS attacks.

6) Security and Privacy Support for DCS: The application demand has led to the development of data centric sensor networks (DCS), where the sensor data as contrast to sensor nodes are named based on attributes such as event type or geographic location. To address the security problems of DCS, Shao, et al. in [150] present *p*DCS, a privacy-enhanced DCS network which offers different levels of data privacy based on different cryptographic keys. *p*DCS offers different levels of location privacy and allow a tradeoff between privacy and query efficiency. In addition, they propose several query optimization techniques based on Euclidean Steiner Tree [151] and Keyed Bloom Filter [152] to minimize the query overhead while providing certain query privacy.

7) Node Compromise Distribution Modeling: Node compromise is the major problem in sensor networks that leads to internal attacks. It is obvious that knowing the probability of node compromise with a given time and position can help a system monitor, identify and defend against node compromise efficiently and effectively. Based on whether the network has node compromise detecting mechanisms, Chen, et al. in [69] classify node compromise distribution models as basic models or intelligent models. Basic models can further be divided as basic uniform models and basic gradient models. Intelligent models can further be divided as intelligent uniform models and intelligent gradient models. These models allow systems to estimate the probability of node compromise. The difference between a uniform model and a gradient model is that the location of a sensor may affect the node compromise probability in the latter model, while it does not matter in the previous model. The difference between a basic model and an intelligent model is that: the latter model considers the effect of compromise events come from neighbor nodes when estimating the probability of node compromise. Applying these models in system security designs can improve system security and decrease the overheads in nearly every security area including key management, secure routing, and node compromise detection.

B. Summary

Security assessment, data assurance, survivability, trust evaluation, end-to-end security, security and privacy support, node compromise distribution, etc. are also important in sensor network security. Until now, there have been only a few approaches available, and more studies are needed in these areas.

XI. Summary

Security in sensor networks is a new area of research, with a limited, but rapidly growing set of research results. Because of its linchpin in some application areas, it is worth studying. In this paper, we present a nearly comprehensive survey of security researches in wireless sensor networks, which has been presented in the literature.

We summarize security challenges and analyze threats and attacks. Based on the network protocol model, we review nearly all types of crippling attacks against the functions of protocol layers. We also provide summarization of countermeasures and design considerations. Then we review seven major issues in securing WSNs and also proposed our suggestions:

- Cryptography: Cryptography Selection is fundamental to providing security services in WSNs. Most security approaches adopt symmetric key cryptography, thus introducing complex key management. Although some recent studies show public key cryptography is available for WSNs, private key operations in asymmetric cryptography schemes are still too expensive in terms of computation and energy cost for sensor nodes, and still need further studies.
- Key management: Key management is the linchpin of cryptograph mechanism especially for symmetric key cryptography. After reviewing current approaches, we give our suggestions: adopting symmetric cryptography and one-way hash functions and using a distributed mechanism instead of a centralized mechanism; combining deployment knowledge, location information, and key-predistribution; integrating node identity and key produce; adopting an adaptive re-key mechanism to defend against cryptography attacks; integrating secure resilience and a system application environment; considering network structure, etc.
- Attack detections and preventions: Although most secure schemes are able to limit the effects of attacks, attack detections are still need for system security. In general, most attack detecting mechanisms belong to centralized approaches or neighbors' cooperative approaches. The disadvantage of the first method is that it introduces more routing traffic from the given node to the base station; while the second method introduces more computing process and monitoring tasks for neighbor nodes. In all, Watchdog and Reputation Rating based or Virtual currency methods are able to prevent DoS attacks in some extent. Code testing methods and location verification methods open our eyes to node compromise detection, though they need improvement.
- Secure routing: Many sensor network routing protocols are quite simple and offer little to no security features, and there are some types of attacks that disable routing. Though there are some secure routing protocols for ad hoc networks, figuring out how to adapt them to sensor networks still needs more works. After reviewing current approaches, we give our suggestions: Authentication is required for broadcast; A system should prevent adversaries from knowing the network topology; Multi-path can tolerate routing attacks to some extent; Routing information should be encrypted; Identifying malicious nodes and isolating them from routing path will improve system security performance; Integrating location information can help a routing path immune spoof; Using localized algorithms instead of centralized ones will improve system performance; Using the special structure of cluster or hierarchical sensor networks can provide more efficient secure routing algorithm; Base station protection needs more considerations; Reduce overhead when possible; etc.
- Security location: Providing reliable and accurate location or position information is the key factor in some sensor networks when position or location information is the object of these networks, or if they use distance or geography routing algorithms. To provide location security, we can adopt multiple verifications to detect or tolerate attacks in beacon detecting location mechanisms. In a group membership estimating location mechanism, we can use the statistical method and deployment knowledge to secure location.
- Secure data fusion: Data fusion security issues can occur in the original sensors, intermediate nodes, and the aggregators. To provide security, we can adopt authentication, neighbor nodes' collective endorsement or similar methods to verify the correction of the aggregation reports, or we can use statistical methods to filter the fake data. Some studies suggest that using ciphertext instead of plaintext to prevent the disclosure of data in intermediate nodes, though these methods usually lower the security level.
- Other security issues: Security assessment, data assurance, survivability, trust evaluation, end-to-end security, security and privacy support, node compromise distribution, etc. are also important in sensor network security. Until now, there have been only a few approaches available, and more studies are needed in these areas.

As our survey shows, there are several unsolved research problems that deserve more attention:

- Inexpensive private key operations on sensor nodes: Though some studies show that asymmetric key cryptography can be used to secure WSNs, improving the efficiency of private key operations on sensor nodes is highly desirable.
- Key management for mobile flat WSNs: Most current key management protocols are only suitable for static WSNs.

New protocols for mobile WSNs including mobile nodes and mobile base stations need to be developed.

- Intelligent attack/node compromise detecting mechanism: Most current detecting systems monitor all the nodes in the system without emphasis, and the system should decentralize their resources evenly in all nodes in order to monitor whether they have larger compromise probabilities or not. That makes the detecting mechanism less efficient. Due to the heavy work, the system performance may decrease largely, and may even make this work unpractical. It is highly desirable to design an efficient and effective mechanism that chooses those nodes with larger probabilities of being attacked as the main monitoring objects.
- Secure routing for mobile WSNs: Most current secure routing algorithms assume the sensor network is stationary. It is highly needed to study secure routing protocols for mobile WSNs.
- Secure routing to defend against undetected attacks: Currently, there are some protocols that let routing paths bypass the detected compromised nodes or attacks. However, most compromise activities can not be immediately detected because any detecting mechanism needs time and the fraudulent action of adversaries (adversaries don't want system to notice their attacking activities, thus they will adopt any action that one can imagine to make the detecting time longer.) makes the time even longer. Consequently, current secure routing algorithms have no effect to conquer undetected attacks. New secure routing protocols that can defend against undetected attacks or node compromise are highly desirable.
- Security and QoS: Most current security studies focus on individual topics of security issues. However, security overhead will degrade other performances of WSNs. The tradeoff between security and QoS needs to be evaluated.
- Base station protection: Most approaches assume the base station is secure and robust enough. However, in some special application environment, such as battlefield surveillance, base stations may be easy to be destroyed or attacked. Under such conditions, base station protection and the other issues that are introduced by the base station protection must be carefully investigated.

REFERENCES

[1] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proc. International Conf. Mobile Computing Networking*, 1999, pp. 263–270.

[2] J. W. Gardner, V. Varadan, and O. Awadelkarim, *Microsensors, MEMS and Smart Devices*. New York: Wiley, 2001.

[3] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for network sensors," in *Proc. ASPLOS-IX*, 2000.

[4] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for "smart dust," in *Proc. International Conf. Mobile Computing Networking*, 1999, pp. 271–278.

[5] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, pp. 102–114, 2002.

[6] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Commun. Mag.*, vol. 11, pp. 38–43, 2004.

[7] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Commun. Surveys Tutorials*, vol. 7, pp. 2–28, 2005.

[8] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys Tutorials*, vol. 8, pp. 2–23, 2006.

[9] A. S. Tanenbaum, *Computer Networks*, 4th ed. NJ: Prentice Hall, 2003.

[10] W. Stallings, *Cryptography and Network Security- Principles and Practices*, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2003.

[11] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," NAI Labs Technical Report 00-010, 2000.

[12] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, Special Issue: Wireless sensor networks, vol. 47, pp. 53–57, 2004.

[13] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, pp. 54-62, 2002.

[14] H. Song, L. Xie, S. Zhu, and G. Cao, "Sensor node compromise detection: The location perspective," in *Proc. International Conf. Wireless Commun. Mobile Computing*, 2007, pp. 242–247.

[15] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in *Proc. 3rd International Symposium on Information Processing in Sensor Networks*, 2004, pp. 259–268.

[16] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symposium Security Privacy*, 2003, pp. 197–213.

[17] B. Deb, S. Bhatnagar, and B. Nath, "Information assurance in sensor networks," in *Proc. 2nd ACM International Conference on Wireless Sensor Networks and Applications*, 2003, pp. 160–168.

[18] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Elsevier's AdHoc Networks Journal*, Special Issue on Sensor Network Applications and Protocols, vol. 1, pp. 293–315, 2003.

[19] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proc. *2nd ACM International Conf. Wireless Sensor Networks Applications*, 2003, pp. 151–159.

[20] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Springer Netherlands Wireless Networks*, vol. 8, pp. 521–534, 2002.

[21] Y. W. Law, J. Doumen, and P. Hartel, "Benchmarking block ciphers for wireless sensor networks," in *Proc. IEEE International Conf. Mobile Ad-hoc Sensor Systems*, 2004, pp. 447–456.

[22] Y. W. Law, J. Doumen, and P. Hartel,"Survey and benchmark of block ciphers for wireless sensor networks," *ACM Trans. Sensor Networks*, vol. 2, pp. 65–93, 2006.

[23] D. Malan, "Crypto for tiny objects," Harvard University TR-04-04, 2004.

[24] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, "State of the art in public-key cryptography for wireless sensor networks," in *Proc. 3rd IEEE International Conf. Pervasive Computing Commun. Workshops (PERCOMW)*, 2005, pp. 146–150.

[25] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyOS based on elliptic curve cryptography," in *Proc. 1st IEEE International Conf. Sensor Ad Hoc Commun. Networks SECON*, 2004, pp. 71–80.

[26] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public key cryptography in sensor networks-revisited," in Proc. *1st European Workshop Security Ad-Hoc Sensor Networks (ESAS)*, 2004.

[27] M. Bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in *Proc. ACM Workshop Wireless Security*, 2003, pp. 79–87

[28] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. 2nd International Conference on Embedded Networked Sensor Systems*, 2004, pp. 162–175

[29] S. Schmidt, H. Krahn, S. Fischer, and D. Watjen, "A security architecture for mobile wireless sensor networks," in *Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS)*, 2004.

[30] K. Yuksel, J.-P. Kaps, and B. Sunar, "Universal hash functions for emerging ultra-low-power networks," in *Proc. Commun. Networks Distributed Systems Modeling Simulation Conf. (CNDS)*, 2004.

[31] I. C. Technology, "MICA2: Wireless Measurement System."

[32] S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: A survey," Computer Science Department at RPI Tech, Rep. TR-05-07, 2005.

[33] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. Conf. Computer Commun. Security*, 2002, pp. 41–47.

[34] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Trans. Inform. System Security (TISSEC)*, vol. 8, pp. 228–258, 2005.

[35] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Trans. Inform. System Security (TISSEC)*, vol. 8, pp. 41–77, 2005.

[36] F. Delgosha and F. Fekri, "Threshold key-establishment in distributed sensor networks using a multivariate scheme," in *Proc. IEEE INFOCOM*, 2006.

[37] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach," in *Proc. 11th IEEE International Conf. Network Protocols Center Secure Inf. Syst.*, 2003, pp. 326–335.

[38] R. D. Pietro, L. V. Mancini, and A. Mei, "Random key assignment for secure wireless sensor networks," in *Proc. 1st ACM Workshop Security Ad hoc Sensor Networks*, 2003, pp. 62–71

[39] F. Anjum, "Location dependent key management using random key-predistribution in sensor networks," in *Proc. 5th ACM Workshop on Wireless Security*, 2006, pp. 21–30

[40] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. IEEE INFOCOM*, 2004

[41] D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key management scheme for wireless sensor networks," in *Proc. 2nd ACM Sorkshop on Security of Ad hoc and Sensor Networks*, 2004, pp. 29–42

[42] D. Liu and P. Ning, "Location-based pairwise key establishments for static sensor networks," in *Proc. 1st ACM Workshop on Security of Ad hoc and Sensor Networks*, 2003, pp. 72–82.

[43] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in *Proc. 6th ACM International Symposium Mobile Ad hoc Networking Computing (MOBIHOC)*, 2005, pp. 34–45

[44] H. Chan and A. Perrig, "PIKE: Peer intermediaries for key establishment," in *Proc. IEEE INFOCOM*, 2005.

[45] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor hetworks," in *Proc. 10th ACM Conf. Computer Commun. Security*, 2003 pp. 62–72.

[46] L. Zhou, J. Ni, and C. V. Ravishankar, "Supporting secure communication and data collection in mobile sensor networks," in *Proc. IEEE INFOCOM*, 2006.

[47] J. Lee and D. R. Stinson, "Deterministic key predistribution schemes for distributed sensor networks." vol. 3357/2004: Springer Berlin / Heidelberg, 2004, pp. 294–307.

[48] J. Lee and D. R. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks," in *Proc. IEEE Wireless Commun. Networking Conf.*, 2005, vol. 2, pp. 1200–1205.

[49] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in *Proc. 2nd ACM International Conf. Wireless Sensor Networks Applications*, 2003, pp. 141–150.

[50] J. Zachary, "A decentralized approach to secure group membership testing in distributed sensor networks," in *Proc. IEEE Military Commun. Conf.*, 2003.

[51] R. Dutta and S. Mukhopadhyay, "Improved self-healing key distribution with revocation in wireless sensor network," in *Proc. IEEE Wireless Commun. Networking Con.(WCNC)*, 2007, pp. 2963–2968.

[52] W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," in *Proc. 6th ACM International Symposium Mobile Ad Hoc Networking Computing (MobiHoc)*, 2005.

[53] C.-H. Huang and D. Du, "New constructions on broadcast encryption and key pre-distribution schemes," in *Proc. IEEE INFOCOM*, 2005.

[54] W. Zhang and G. Cao, "Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach," in *Proc. IEEE INFOCOM*, 2005.

[55] R. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in *Proc. 12th IEEE International Conf. Network Protocols (ICNP)*, 2004.

[56] M. J. Miller and N. H. Vaidya, "Leveraging channel diversity for key establishment in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2006.

[57] M. Chorzempa, J. M. Park, and M. Eltoweissy, "SECK: Survivable and efficient keying in wireless sensor networks," in *Proc. IEEE Workshop Information Assurance Wireless Sensor Networks, (WSNIA)*, 2005.

[58] M. Eltoweissy, M. Younis, and K. Ghumman, "Lightweight key management for wireless sensor networks," in *Proc. IEEE International Conf. Performance, Computing, Commun.*, 2004, pp. 813–818.

[59] Y.-S. Jeong, B.-K. Lee, and S.-H. Lee, "An efficient key management scheme for secure sensor networks," in *Proc. 6th IEEE International Conf. Computer Inform. Technol. (CIT)*, 2006, p. 228.

[60] G. Jolly, M. Kuscu, P. Kokate, and M. Youni, "A low-energy key nanagement protocol for wireless sensor networks," in *Proc. 8th International Symposium Computers Commun. (ISCC)*, 2003, vol. 1, pp. 335–340.

[61] M. F. Younis, K. Ghumman, and M. Eltoweissy, "Location-aware combinatorial key management scheme for clustered sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 17, pp. 865–882, 2006.

[62] P. Traynor, H. Choi, G. Cao, S. Zhu, and T. L. Porta, "Establishing pair-wise keys in heterogeneous sensor networks," in *Proc. IEEE INFOCOM*, 2006.

[63] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Two-layered dynamic key management in mobile and long-lived cluster-based wireless sensor networks," in *Proc. IEEE Wireless Commun. Networking Conf. (WCNC)*, 2007, pp. 4145–4150.

[64] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti, "Secure pebblenets," in *Proc. 2nd ACM International Symposium on Mobile Ad hoc Networking Computing*, 2001, pp. 156–163.

[65] R. D. Pietro, L. V. Mancini, Y. W. Law, S. Etalle, and P. J. M. Havinga, "LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks," in *Proc. International Conf. Parallel Processing Workshops*, 2003, pp. 397–406.

[66] R. Anderson and M. Kuhn, "Tamper resistance - A cautionary note," in *Proc. 2nd USENIX Workshop Electronic Commerce*, 1996, pp. 1–11.

[67] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. EUROCRYPT 84 Workshop Advances Cryptology*. New York: Springer-Verlag 1985, pp. 335–338.

[68] B. Dutertre, S. Cheung, and J. Levy, "Lightweight key management in wireless sensor networks by leveraging Initial trust," System Design Laboratory 2004.

[69] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Node compromise modeling and its applications in sensor networks," in *Proc. IEEE Symposium Computers Communications (ISCC)*, 2007.

[70] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," in *Proc. IEEE INFOCOM*, 2003.

[71] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proc. 3rd ACM Workshop Wireless Security*, 2004, pp. 51–60.

[72] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symposium Security and Privacy*, 2005, pp. 49–63.

[73] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2007, pp. 1307–1315.

[74] C. Jaikaeo, C. Srisathapornphat, and C.-C. Shen, "Diagnosis of sensor networks," in *Proc. IEEE International Conf. Commun.*, 2001, vol. 5, pp. 1627–1632.

[75] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in *Proc. 1st ACM International Workshop Wireless Sensor Networks Applications*, 2002, pp. 122–130

[76] G. Wang, W. Zhang, and G. Cao, "On supporting distributed collaboration in sensor networks," in *Proc. IEEE Military Communi. Conf.*, 2003, vol. 2, pp. 752–757.

[77] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annual International Conference Mobile Computing Networking*, 2000, pp. 255–265

[78] M. Ding, D. Chen, K. Xing, and X. Cheng, "Localized fault-tolerant event boundary detection in sensor networks," in *Proc. IEEE INFOCOM*, 2005, vol. 2, pp. 902–913

[79] B. Krishnamachari and S. Iyengar, "Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks," *IEEE Trans. Comput.*, vol. 53, pp. 241–250, 2004.

[80] T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos, "Distributed deviation detection in sensor networks," *ACM SIGMOD Record*, vol. 32, pp. 77–82, 2003.

[81] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2007, pp. 1937–1945.

[82] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. Advanced Commun. Multimedia Security*, 2002, pp. 107–121.

[83] S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in *Proc. 10th Euromicro Workshop Parallel, Distributed Network-Based Processing*, 2002, pp. 403–410.

[84] P. Michiardi and R. Molva, “Simulation-based analysis of security exposures in mobile ad hoc networks,” in *Proc. European Wireless 2002: Next Generation Wireless Networks: Technologies, Protocols, Services Applications*, 2002.

[85] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J.-P. Hubaux, and J.-Y. L. Boudec, “Self-organization in mobile ad hoc networks: The approach of terminodes,” *IEEE Commun. Mag.*, vol. 39, pp. 166–174, 2001.

[86] L. Buttyan and J.-P. Hubaux, “Nuglets: A virtual currency to stimulate cooperation in self-organized mobile ad hoc networks,” Swiss Federal Institute of Technology 2001.

[87] S. Zhong, J. Chen, and Y. R. Yang, “Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks,” in *Proc. IEEE INFOCOM*, 2003, vol. 3, pp. 1987–1997

[88] A. Seshadri, A. Perrig, L. v. Doorn, and P. Khosla, “SWATT: SoftWare-based ATTestation for embedded devices,” in *Proc. IEEE Symposium Security Privacy*, 2004, pp. 272–282.

[89] A. Seshadri, M. Luk, A. Perrig, L. v. Doorn, and P. Khosla, “SCUBA: Secure code update by attestation in sensor networks,” in *Proc. 5th ACM Workshop Wireless Security*, 2006, pp. 85–94.

[90] R. Sailer, X. Zhang, T. Jaeger, and L. v. Doorn, “Design and implementation of a TCG-based integrity measurement architecture,” in *Proc. 13th USENIX Security Symposium*, vol. 13, IBM T. J. Watson Research Center, 2004.

[91] C. Krauss, F. Stumpf, and C. Eckert, “Detecting node compromise in hybrid wireless sensor networks Using attestation techniques,” in *Proc. Security and Privacy in Ad-hoc and Sensor Networks*, vol. 4572/2007. Springer: Berlin/Heidelberg, 2007.

[92] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, “Denial-of-service attacks on battery-powered mobile computers,” in *Proc. 2nd IEEE Annual Conf. Pervasive Computing Commun. (PerCom)*, 2004, pp. 309–318.

[93] J. M. McCune, E. Shi, A. Perrig, and M. K. Reiter, “Detection of denial-of-message attacks on sensor network broadcasts,” in *Proc. IEEE Symposium Security Privacy*, 2005, pp. 64–78.

[94] A. A. Pirzada and C. McDonald, “Secure routing with the AODV protocol,” in *Proc. Asia -Pacific Conf. Commun.*, 2005.

[95] S. Bhargava and D. P. Agrawal, “Security enhancements in AODV protocol for wireless ad hoc networks," in *Proc. 54th IEEE Vehicular Technology Conference*, 2001, vol. 4, pp. 2143–2147.

[96] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, “URSA: Ubiquitous and robust access control for mobile ad hoc networks,” *IEEE/ACM Trans. Networking*, vol. 12, pp. 1049–1063, 2004.

[97] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A secure routing protocol for ad hoc networks,” in *Proc. 10th IEEE International Confe. Network Protocols*, 2002, pp. 78–87.

[98] P. Papadimitratos and Z. J. Haas, “Secure routing for mobile ad hoc networks,” in *Proc. SCS Commun. Networks Distributed Systems Modeling Simulation Conf.*, 2002

[99] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, “An on-demand secure routing protocol resilient to byzantine failures,” in *Proc. ACM Workshop on Wireless Security*, 2002, pp. 21–30.

[100] A. Woo, T. Tong, and D. Culler, “Taming the underlying challenges of reliable multihop routing in sensor networks,” in *Proc. 1st International Conf. Embedded Networked Sensor Systems*, 2003, pp. 14–27.

[101] J. Deng, R. Han, and S. Mishra, “INSENS: Intrusion-tolerant routing in wireless sensor networks,” *Computer Commun.*, vol. 29, pp. 216–230 2006.

[102] J. Deng, R. Han, and S. Mishra, “Enhancing base station security in wireless sensor networks,” University of Colorado Technical Report, CU-CS-951-03, 2003.

[103] J. Deng, R. Han, and S. Mishra, “A performance evaluation of intrusion tolerant routing in wireless sensor networks,” in *Proc. 2nd International Workshop Information Processing Sensor Networks (IPSN)*, 2003, pp. 349–363.

[104] C. Karlof, Y. Li, and J. Polastre, “ARRIVE: Algorithm for robust routing in volatile environments,” Technical Report UCB/CSD-03-1233, University of California at Berkeley, 2002.

[105] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, “SIGF: A family of configurable, secure routing protocols for wireless sensor networks,” in *Proc. 4th ACM Workshop Security of Ad hoc Sensor Networks*, 2006, pp. 35–48

[106] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, “Feedback: Towards dynamic behavior and secure routing for wireless sensor networks,” in *Proc. 20th International Conf. Advanced Information Networking Applications (AINA)*, 2006, vol. 2, pp. 160–164.

[107] K.-S. Hung, K.-S. Lui, and Y.-K. Kwok, “A trust-based geographical routing scheme in sensor networks,” in *Proc. IEEE Wireless Commun. Networking Conf. (WCNC)*, 2007, pp. 3123–3127.

[108] M. Tubaishat, J. Yin, B. Panja, and S. Madria, “A secure hierarchical model for sensor network,” *ACM SIGMOD Record*, vol. 33, pp. 7–13, 2004.

[109] D. Liu and P. Ning, “Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks,” in *Proc. 10th Annual Network Distributed System Security Symposium (NDSS)*, 2003, pp. 263–276.

[110] S. S. Al-Wakeel and S. A. AL-Swailem, “PRSA: A path redundancy based security algorithm for wireless sensor networks,” in *Proc. IEEE Wireless Commun. Networking Conf. (WCNC)*, 2007, pp. 4156–4160.

[111] D. An and H. Cam, “Route recovery with one-hop broadcast to bypass compromised nodes in wireless sensor networks,” in *Proc. IEEE Wireless Commun. Networking Conf. (WCNC)*, 2007, pp. 2495–2500.

[112] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, “Protecting receiver-location privacy in wireless sensor networks,” in *Proc. IEEE INFOCOM*, 2007, pp. 1955–1963.

[113] J. Yin and S. Madria, “SecRout: A secure routing protocol for sensor networks,” in *Proc. 20th International Conf. Advanced Information Networking Applications (AINA)*, 2006, vol. 1, pp. 393–398.

[114] S. Capkun and J.-P. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” in *Proc. INFOCOM*, 2005, vol. 3, pp. 1917–1928

[115] L. Lazos and R. Poovendran, “SeRLoc: Secure range-independent localization for wireless sensor networks,” in *Proc. 3rd ACM Workshop Wireless Security*, 2004, pp. 21–30.

[116] N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” in *Proc. 2nd ACM Workshop Wireless Security*, 2003, pp. 1–10.

[117] Z. Li, W. Trappe, Y. Zhang, and B. Nath, “Robust statistical methods for securing wireless localization in sensor networks,” in *Proc. 4th International Symposium Information Processing in Sensor Networks*, 2005.

[118] S. Capkun, M. Cagalj, and M. Srivastava, “Secure localization with hidden and mobile base stations,” in *Proc. IEEE INFOCOM*, 2006.

[119] Y. Chen, W. Trappe, and R. P. Martin, “Attack detection in wireless localization,” in *Proc. IEEE INFOCOM*, 2007.

[120] J. Hwang, T. He, and Y. Kim, “Detecting phantom nodes in wireless sensor networks,” in *Proc. IEEE INFOCOM*, 2007, pp. 2391–2395.

[121] D. Liu, P. Ning, and W. Du, “Detecting malicious beacon nodes for secure location discovery in wireless sensor networks,” in *Proc. 25th International Conf. Distributed Computing Systems (ICDCS)*, 2005, pp. 609–619.

[122] D. Liu, P. Ning and W. Du, “Attack-resistant location estimation in sensor networks," in *Proc. 4th International Symposium Information Processing Sensor Networks*, 2005, pp. 99- 106.

[123] L. Fang, W. Du, and P. Ning, “A beacon-less location discovery scheme for wireless sensor networks,” in *Proc. IEEE INFOCOM*, 2005.

[124] W. Du, L. Fang and P. Ning, “LAD: Localization anomaly detection for wireless sensor networks,” in *Proc. 19th IEEE International Parallel Distributed Processing Symposium*, 2005, pp. 41a–41a.

[125] S. Brands and D. Chaum, “Distance-bounding protocols,” in *Proc. Adv. Cryptology - EUROCRYPT ’93: Workshop Theory Application Cryptographic Techniques*, vol. 765/1994. Springer Berlin / Heidelberg, 1994, pp. 344–359.

[126] L. Hu and D. Evans, “Secure aggregation for wireless networks,” in *Proc. Symposium Applications Internet Workshops*, 2003, pp. 384–391.

[127] J. Deng, R. Han, and S. Mishra, “Security support for in-network processing in wireless sensor networks,” in *Proc. 1st ACM Workshop Security Ad hoc Sensor Networks*, 2003, pp. 83–93.

[128] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A witness-based approach for data fusion assurance in wireless sensor networks,” in *Proc. IEEE Global Telecommun. Conf.*, 2003, vol. 3, pp. 1435–1439

[129] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure information aggregation in sensor networks,” in *Proc. 1st International Conf. Embedded Networked Sensor Systems*, 2003, pp. 255–265.

[130] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks,” in *Proc. IEEE Symposium Security Privacy*, 2004, pp. 259–271.

[131] H. Vogt, “Exploring message authentication in sensor networks,” in *Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS)*, 2004.

[132] Z. Yu and Y. Guan, “A dynamic en-route scheme for filtering false data injection in wireless sensor networks,” in *Proc. IEEE INFOCOM*, 2006.

[133] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE J. Select. Areas Commun.*, vol. 23, pp. 839–850, 2005.

[134] D. Wagner, "Resilient aggregation in sensor networks," in *Proc. 2nd ACM Workshop Security Ad hoc Sensor Networks*, 2004, pp. 78–87.

[135] J. Girao, D. Westhoff, and M. Schneider, "CDA: Concealed data aggregation in wireless sensor networks," in *Proc. ACM WiSe*, 2004.

[136] S. Peter, K. Piotrowski, and P. Langendoerfer, "On concealed data aggregation for WSNs," in *Proc. 4th IEEE Consumer Communi. Networking Conf. (CCNC)*, 2007, pp. 192–196.

[137] J. Domingo-Ferrer, "A provably secure additive and multiplicative privacy homomorphism" in *Proc. Information Security Conf.*, 2002, pp. 471–483.

[138] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," in *Proc. Foundations Secure Computation*, 1978, pp. 169–179.

[139] D. Wagner, "Cryptanalysis of an algebraic privacy homomorphism," in *Proc. 6th Information Security Conf. (ISC)*, 2003.

[140] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proc. 2nd International Conf. Mobile Ubiquitous Systems: Networking Services (MobiQuitous)*, 2005, pp. 109–117.

[141] Y. W. Law, S. Etalle, and P. H. Hartel, "Assessing security in energy-efficient sensor networks," in *Proc. 18th IFIP TC11 Int. Conf. Information Security Privacy Age Uncertainty (SEC)*, 2003, pp. 459–463.

[142] Y. W. Law, S. Dulman, S. Etalle, and P. Havinga, "Assessing security-critical energy-efficient sensor networks," Univ. of Twente, The Netherlands, Tech. Rep. TR-CTIT-02-18 2002.

[143] X. Li and D. Yang, "A quantitative survivability evaluation model for wireless sensor networks," in *Proc. IEEE International Conf. Networking, Sensing Control (ICNSC)*, 2006, pp. 727–732.

[144] D. S. Kim, S. KM, and J. S. Park, "A framework of survivability model for wireless sensor network," in *Proc. 1st International Conf. Availability, Reliability Security (ARES)*, 2006, pp. 515–522.

[145] S. Kumar, R. Valdez, O. Gomez, and S. Bose, "Survivability evaluation of wireless sensor network under DDoS attack," in *Proc. International Conf. Networking; International Conf. Systems; International Conf. Mobile Commun. Learning Technologies (ICN/ICONS/MCL)*, 2006, pp. 23–29.

[146] G. W. Skelton and A. Holton, "Survivability in wireless sensor networks," in *Proc. IEEE SoutheastCon*, 2006, pp. 341-341.

[147] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proc. IEEE INFOCOM*, 2006.

[148] G. V. Crosby and N. Pissinou, "Cluster-based reputation and trust for wireless sensor networks," in *Proc. 4th IEEE Consumer Commun. Networking Conf. (CCNC)*, 2007, pp. 604–608.

[149] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2006.

[150] M. Shao, S. Zhu, W. Zhang, and G. Cao, "pDCS: Security and privacy support for data-centric sensor networks," in *Proc. IEEE INFOCOM*, 2007, pp. 1298–1306.

[151] P. Winter and M. Zachariasen, "Euclidean steiner minimum trees: An improved exact algorithm," *Networks*, vol. 30, pp. 149–166, 1997.

[152] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, no. 7, pp. 422–426, 1970.

Xiangqian Chen received his PhD at the Department of Electrical and Computer Engineering, Florida International University in December 2007. His research interests include wireless and mobile computing, wireless communications, network security, and ad hoc and sensor networks.

Kia Makki is a full professor of Telecommunications and Information Technology Institute at Florida International University, USA. He received the PhD degree in Computer Science from the University of California, Davis in 1988. His current research interests include computer and information security, wireless communication, and security for ad hoc and sensor networks. He has served in different capacities for various journals and conferences.

Kang Yen is a full professor and the chairperson of the Electrical and Computer Engineering department at Florida International University. He received the PhD degree from Vanderbilt University in 1985. His research interests include system modeling and simulation, control theory, parallel processing, microprocessor and AI applications.

Niki Pissinou is a full professor and the director of the Telecommunications and Information Technology Institute at Florida International University, USA. Her current research interests include computer and information security, wireless communication, and mobile computing.