Authentication and Integrity of Data in Wireless Sensor Network with Mobile Sink

P. M. Kakade
Department of Computer Engineering,
STES's Smt. Kashibai Navale College of Engineering,
Pune-41, India.

V. V. Kimbahune
Department of Computer Engineering,
STES's Smt. Kashibai Navale College of Engineering,
Pune-41, India.

ABSTRACT
The Wireless Sensor Network (WSN) is one of the core technologies to form the future networks. As WSN consisting of several sink nodes and sensor nodes, while it have many advantages, such as the compact size and the low cost, corresponding constraints on resources can result. The greatest challenge among all is that distinguishing and revoking compromised sensors. Traditional techniques are used for keys pre-distributed among the sinks and sensors for pair wise key establishment and authentication. But this is not that much effective to provide authentication and due to this reason nodes are compromised. To overcome above mentioned problem, new framework was designed. The basic work in it is that to allow a three-tier general framework, use of any pair wise key pre-distribution scheme. The scheme requires two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Keys from this pool are used to strengthened the authentication mechanism between sink and node. For enhancing this, one way chain applied on pre-distributed password. This process has low computational cost and will increase the network resilience. In this process, there is possibility of actual data compromise and sink will not get requested data. Thereby employed, message digests to achieve data integrity by applying complex math on data to ensure that this data has not been tampered with on route to its final destination. Through detailed analysis, we will show that integrity of whole framework improves and assures the accuracy and consistency of data over its entire lifecycle.

General Terms
Security, Node authentication, Integrity of data

Keywords
Wireless sensor network, One way hash chain, Message Digest

1. INTRODUCTION
Security, trust, and authentication are important issues for wireless sensor networks, especially as they become more widely used for industrial control and monitoring applications [2]. A WSN is typically composed of numerous tiny energy-constrained sensor nodes with limited information processing and data storage capabilities. As the wireless sensor networks consist of number of nodes, that nodes are of low power, low cost and which communicate wirelessly, having capability of sensing, processing and communication. Often that sensed data is needed to send back to base station for analysis. Communication between sensor and base station increases distance and results in more energy consumption by which network lifetime reduces.

In many cases sensors containing critical information which are transmitted over network. For this reason security becomes important factor while communicating over network. So security services are needed such as authentication and pair wise key establishment [5]. Traditional system such asymmetric key used for maintaining security but keys used in communication are having high cost for storage. In this process computation cost becomes high. In this case we need to discover some new technique which is having low storage and computational cost.

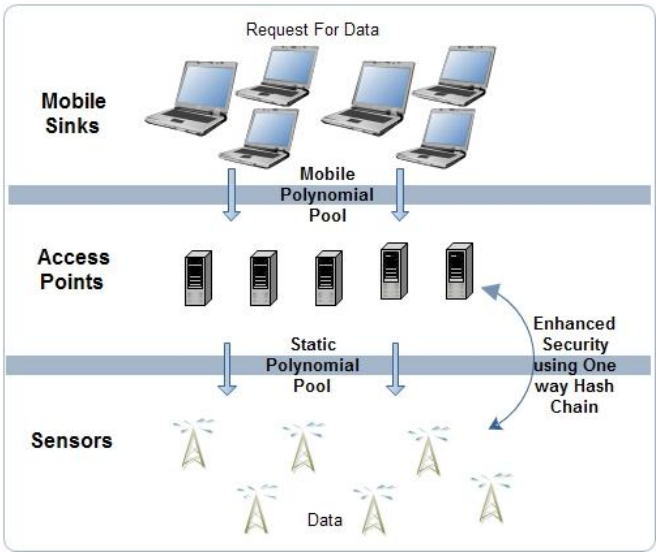

Figure 1: Three tier security framework

For this reason new framework was developed that permits the use of any pair wise key pre-distribution scheme as its basic tool to provide node authentication and pair wise key establishment between sensor nodes and MS's. This framework is also known as three tier security framework shown in figure 1.In the new security framework [1], a small fraction of the preselected sensor nodes which are called as stationary access nodes, that act as authentication access points to the network that trigger the sensor nodes to transmit their aggregated data to mobile sinks. A mobile sink sends data request messages to the sensor nodes via a stationary access node. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial pool are used to establish the authentication between mobile sinks (MS) and stationary access nodes (SAN), which will enable these mobile sinks to access the sensor network for data gathering. Polynomials from the static polynomial pool are used to ascertain the authentication and keys setup between the sensor nodes (SN)

and stationary access nodes. The keys can be distributed in the pool by using polynomial pool based key pre-distribution technique. After key pre-distribution, mobile sink sends request to sensor node for data. This request is forwarded to the mobile sink specified by senor node. In this process path is established between sensor node and mobile sink by matching the key pair. First key pair is matched between SN and SAN, after this it is matched SAN and MS. This establishes secure path between themselves that means only authenticated nodes can communicate in the network. The advantage of using separate pools is that mobile sink authentication is independent of the key distribution scheme used to connect the sensor network. To make the three-tier security scheme more robust against attack, we have strengthened the authentication mechanism between the stationary access nodes and sensor nodes using one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme considered as enhanced three tier security. Mobile sink receives secure data only when it is assured that the data is secure. For this reason integrity of data is maintained by using message digest SHA-2 which is cryptographic hash function and that is resistant to computational attacks.

2. MOTIVATION

There are different security schemes which provide authentication and pair wise keys establishment between communicating nodes. These security schemes usually offer network tolerance to nodes capture. They were widely known as general key agreement schemes, there are three types of general key agreement schemes:

1. Trusted-server scheme

2. Self-enforcing scheme

3. Key pre-distribution scheme

The trusted-server scheme uses a trusted server which is responsible for key agreement between nodes & this type of scheme is not suitable for sensor networks. So there is no trusted infrastructure in sensor networks. Next scheme is self-enforcing scheme which depends on asymmetric cryptography, such as key agreement using public key certificates. This scheme is having limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms. The third type of key agreement scheme is key pre-distribution [5], [6], [7], [8], [10], [11], [12] where before deployment key information is distributed among all sensor nodes.

The simplest scheme of key pre-distribution is to use a global pre-shared among the MS and sensor nodes. This scheme is not favorable against node capture and mobile sink replication attack also offer very low network resilience. Since the capture of a single sensor will lead an attacker to get hold of the pre-shared key and then be able to lunch a wide range network mobile sink replication attack. Eschenauer and Gilgor [5] proposed a more robust scheme against node capture known as probabilistic key pre-distribution scheme.

Before deployment a set of keys was randomly given to each sensor node from static pool. The same static pool was maintained so there is possibility of sharing atleast one common key. So any two sensors have a certain probability of sharing at least one common key. Chan et al. [6], [8] further this idea was extended and designed two key pre-distribution schemes, that are Q-composite key pre-distribution scheme and random pair wise keys scheme. The Q-composite key pre-distribution scheme also uses a key pool but requires two sensor nodes compute a pair wise key from at least Q pre-distributed keys they share. The random pair wise keys scheme randomly picks pairs of sensor nodes and assigns each pair a unique random key. Both schemes improve the security over the basic probabilistic key pre-distribution scheme. The main drawbacks in both the probabilistic key pre-distribution scheme and the Q-composite scheme are high communication overhead and as the number of compromised nodes increases, the fraction of affected pair wise keys increases quickly. This results in, small fraction of compromised nodes may compromise large number of keys and that keys are in pair.

An enhanced scheme using the t-degree bivariate key polynomial was proposed by Liu and Ning [7]. They develop a general framework for pair wise key establishment using polynomial pool-based key pre-distribution protocol and the probabilistic key distribution. Their scheme provides higher networks resiliency to nodes capture compared to the global pre-shared key, the probabilistic key pre-distribution scheme, and the Q-composite scheme, it can only tolerate no more than t compromised nodes, where the value of t is limited by the memory available in sensor nodes. Therefore, we consider the polynomial pool-based key pre-distribution scheme as the basic component in our proposed schemes for network resiliency and low communication overhead against nodes capture.

3. RELATED WORK

For authentication there are different basic schemes, which are used to distribute the keys between the nodes but to secure the three tier network framework[1] separate key pools used, one for the mobile sink to access the network, and one for pairwise key establishment between the sensors in which polynomial pool based key pre-distribution technique used. This technique uses a pool of randomly generated polynomials and provides higher network's resiliency to nodes capture, where as in Q composite & random key pre-distribution [6], [8] can only tolerate no more than *t* compromised nodes. For key generation this polynomial plays an important role. With the help of polynomial keys are generated and some pool is maintained which will helpful for authenticating the nodes. Key distribution working within nodes is shown in the figure 2.

The set of keys are given randomly to the node. For node authentication mobile sink and stationary access node matching key pair from their pre-distributed keys likewise same key matching is done between the stationary access node and sensor node. Depending on this secure path will be established in which data will be sent to the mobile sink from sensor node. Enhanced security is provided between sensors by applying one way hash chain on pre-distributed password. For this MD5 one way hash function is used. Data integrity is maintained while sending data.

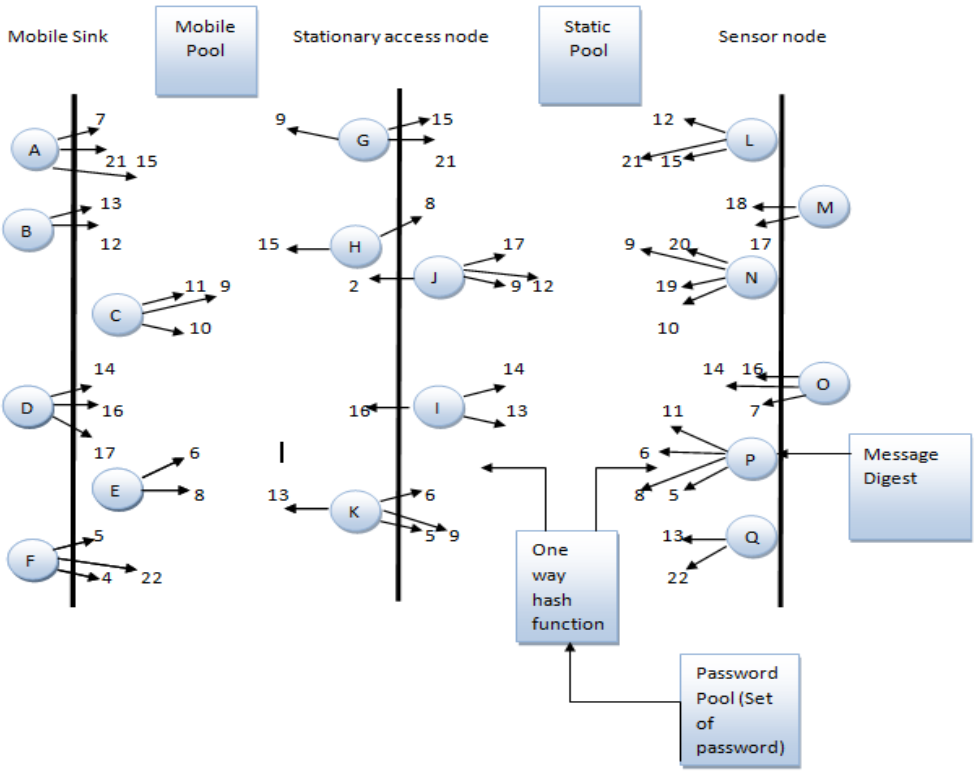

Figure 2: Path establishment

In this, mobile sink can assure about the data which is not replicated, secure and received from requested destination. Message digests achieve data integrity by applying complex math on data to ensure that this data has not been tampered with on route to its final destination.

4. PROPOSED MODEL

Once the nodes are authenticated, with the help of three tier security framework, it is assured that mobile sink can establish secure connection with the sensor can request for the data or any required information. According to request integrated data forwarded back to mobile by sensor node by using message digest. This is one way hash function which provides integrity of data.

4.1 Model

Following figure 3 shows architecture of the proposed system. There are different actors in system such as Mobile sink, sensor node, and stationary access node. First keys are generated by using polynomial pool based key pre-distribution technique and that keys are placed in separate pool. From that pool keys are distributed to nodes. Those pools are mobile pool (|M|) and static pool (|S|). Ks Keys from static pool are given to the sensor node and Ks-1 keys to stationary access node, likewise Km keys given to mobile sink and 1 key given to stationary access node for improving complexity of key guessing for attacker. By using this key secure path is established in which communication is performed.

Enhanced security provided through one way hash function and data integrity through message digest. This message digest class provides applications the functionality of a message digest algorithm, such as SHA-1 or SHA-256. message digests are secure one-way hash functions that take arbitrary-sized data and output a fixed-length hash value. A message digest object starts out initialized. The data is processed through it using the update methods. At any point reset can be called to reset the digest. Once all the data to be updated has been updated, one of the digest methods should be called to complete the hash computation. The digest method can be called once for a given number of updates. After digest has been called, the message digest object is reset to its initialized state. Sha256 is one of the novel one way hash function computed with 32- and 64-bit words, respectively. They use different shift amounts and additive constants. One iteration in a SHA-2 family compression function.

Let, Requested data is D which is having of k bits.

Requirements are,

1. SHA2 (D_S) = HMAC

   where, D_S = Data at sensor node.

2. SHA2 (D_MS) = HMAC

   where, D_MS = Data at Mobile Sink node.

3. Length of HMAC should be 256 bits.

4. HMAC of D_S & HMAC of D_MS should be same.

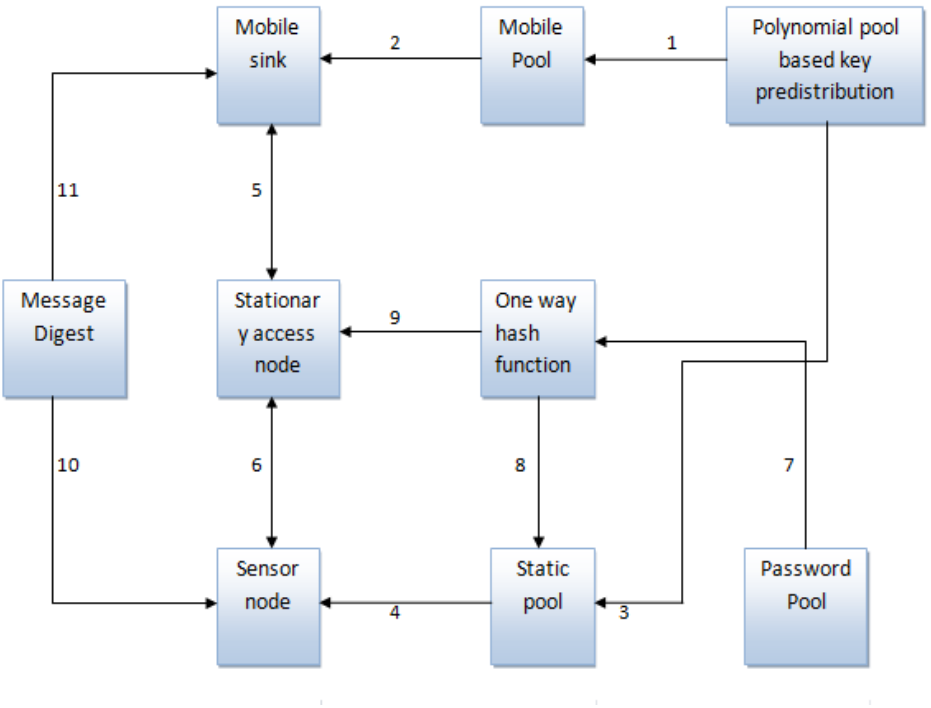

Figure 3: Architecture of system

HMAC (K , m) = H((K ⊕ opad) ‖ H((K ⊕ ipad) ‖ m))

Where,

HMAC is the generated Mac.

K is the Key

M is the message to be encrypted.

⊕ is x-or function.

‖ is the concatenation.

opad is the outer padding (0x5c5c5c…5c5c, one-block-long hexadecimal constant),

ipad is the inner padding (0x363636…3636, one-block-long hexadecimal constant).

4.2 Algorithm

Notation:

Sensor node – u;

Mobile Sink node – v;

Stationary Access Node – a.

Step I. Key Pre-distribution

1. Generate Mobile Polynomial Pool called M of size |M|
2. Generate Static Polynomial Pool called S of size |S|
3. Randomly give K_m (K_m >1) from M to each v
4. Randomly give 1 polynomial from M to each a
5. Randomly give subset of K_s from S to each u
6. Randomly give (K_S -1) from S to each a

Step II. Node identification

7. u finds a such that; a can establish pair wise key with both v & u
   If(direct key establishment)
   {
   1. v sends K_c (encrypted using K_{va}) to a
   2. a receive message & share pair wise key with u
   3. a sends K_c (encrypted using K_{au}) to u

   }
   Else
   {
   1. Find the intermediate sensor node.
   2. Establish pair wise key with help of intermediate sensor node.
   3. Establish direct communication using other sensor node.

   }

Step III. Enhanced 3-tier

8. Generate password based pool W
9. For each u
   {

Randomly choose Gs subset from W
For each Pw_i of Gs
{
Calculate $H^r(Pw_i)$ and load in node u. //r^{th} hash value of Pw^i
}
}

10. For each a
{
Randomly choose Ga subset from W
For each Pw_i of Ga
{
Calculate $H^{r-1}(Pw_i)$ and load in node a. //$r\text{-}1^{th}$ hash value of Pw^i
}
}
11. To match
If (u & a has common static polynomial)
{
Verify a & u such that :
$H(H^{r-1}(Pw_i)) = H^r(Pw_i)$
}

Step IV. Integrity of Data

- Suppose u, a & v are the nodes which share M, S & Wf
- Node u generate the MAC (Message Authentication Code) from Data using SHA2.
- u sends Data with MAC to a
- a forward data with MAC to v.
- v generate MAC from Data.

```
If( Received_MAC == Generated_MAC)
{
    Accept the Data.
}
else{
    Discard the Data.
}
```

5. CONCLUSIONS AND FUTURE WORK

A general three-tier security framework used for authentication and pair wise key establishment between mobile sinks and sensor nodes. It uses polynomial pool-based key pre-distribution scheme which is having pool of polynomials that used to generate set of keys which results, improved network performance compared to the single polynomial pool-based key pre-distribution approach. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network reduces node capture from attacker. Security performance of the stationary access node strengthened by using authentication mechanism between stationary access nodes and sensor nodes. The one-way hash chains algorithm used in conjunction with the static polynomial pool-based scheme and randomly generated passwords is to enhance the authentication.

Further the security performance of the proposed scheme improved with help of message digest SHA-2. This cryptographic one way function applies message authentication code on the data to improve integrity.

6. ACKNOWLEDGMENTS

Idea for the this model referred the IEEE Transaction paper under the title “Three tier security in wireless sensor network with mobile sink” published in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012. This paper contains the results as per given in simulator, are to be implement in real time scenario. authentication code on the data to improve integrity.

7. REFERENCES

[1] Amar Rasheed, and Rabi N. Mahapatra, ”The Three-Tier Security Scheme in Wire-less Sensor Networks with Mobile Sinks” Computer Networks, Volume: 23, Issue: 5.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ”Wireless Sensor Networks: A Survey,” Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[3] J.R. Douceur, ”The Sybil Attack,” Proc. First Int’l Workshop Peer-to- Peer Systems (IPTPS ’02), Mar. 2002.

[4] H. Deng, W. Li, and D.P. Agrawal, ”Routing Security in Wireless Ad Hoc Networks,” Proc. IEEE Comm. Magazine, pp. 70-75, 2002.

[5] L. Eschenauer and V.D. Gligor, ”A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer Comm. Security (CCS ’02), pp. 41-47, 2002.

[6] H. Chan, A. Perrig, and D. Song, ”Random Key Pre-Distribution Schemes for Sensor Networks,” Proc. IEEE Symp. Research in Security and Privacy, 2003. IBM Research Division, Almaden Research Center, 650 Harry Road, San Jose, Ca 95120- 6099.

[7] D. Liu, P. Ning, and R.Li. “Establishing Pair wise Keys in Distributed Sensor Net- works,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp.52-61, Oct. 2003.

[8] H. Chan, A. Perrig, and D. Song, ”Key Distribution Techniques for Sensor Net- works,” Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[9] L. Lamport, ”Password Authentication with Insecure Communication,” Comm. ACM, vol, 24, no. 11, pp. 770-772, Nov. 1981.

[10] S. Zhu, S. Setia, and S. Jajodia, ”LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 62-72, Oct. 2003.

[11] D. Liu and P. Ning, ”Location-Based Pair wise Key Establishments for Static Sensor Networks,” Proc. First ACM Workshop Security Ad Hoc anSensor Networks, 2003

[12] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. o, and M. Yung, “Perfectly-secure key distribution for dynamic conferences,” *Advances in* Cryptology – CRYPTO ’92, LNCS 740, pp. 471-486, 1993.

[13] A. Rasheed and R. N. Mahapatra, **“**A key pre-distribution scheme for heterogeneous sensor networks,” The 5th International Wireless Communications and Mobile Computing Conference (IWCMC’09), pp. 263-268, 2009.