I.J. Information Technology and Computer Science, **2014, 01, 50-56**
Published Online December 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2014.01.06

Energy-efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks

Malika BELKADI
Computer Science Department, Laboratoire de Recherche en Informatique (LARI), Universit é Mouloud Mammeri de Tizi Ouzou, Algeria
E-mail:belkadi_dz@yahoo.fr

Rachida AOUDJIT, Mehammed DAOUI, Mustapha LALAM
Computer Science Department, Laboratoire de Recherche en Informatique (LARI), Universit é Mouloud Mammeri de Tizi Ouzou, Algeria

Abstract— In wireless sensor networks, it is crucial to design and employ energy-efficient communication protocols, since nodes are battery-powered and thus their lifetimes are limited. Such constraints combined with a great number of applications used in these networks, pose many challenges (limited energy, low security…) to the design and management of wireless sensor networks. These challenges necessitate a great attention. In this paper, we present a new version of Directed Diffusion routing protocol which provides both security and energy efficiency together in wireless sensor networks.

Index Terms— Wireless Sensor Networks, Security, Energy efficiency, Directed Diffusion

I. Introduction

Wireless Sensor Networks (WSNs) are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of applications. WSN is composed of densely and usually randomly deploying large number of sensor nodes in a geographical area to monitor its phenomenon and collect its data. The sensed data are then sent to the base station. Sensor nodes are extremely constrained in terms of memory, processor, and energy.

The resources limitation of sensor nodes and the hostile environments, in which they can be deployed, make wireless sensor networks highly vulnerable to several dangerous attacks. Thus, loss of wireless connections may be due to the depletion of the node energy, or simply due to physical destruction by an enemy. Moreover, the lack of security for this type of sensors, and the nature of radio communications increases the risk of attacks on such networks.

Currently, despite these constraints sensor networks are used by many applications such as fire detection, monitoring a patient, homeland security ... Since sensor networks are based on routing protocols to ensure routing sensed data to the base station, it is necessary to consider the security of these protocols as essential criterion. This defines the network's ability to maintain its functionality on increasing its lifetime.

Several routing protocols are developed specifically for sensor networks [1], such as LEACH [2], SPIN [3] and Directed Diffusion (DD) [4]. Directed Diffusion is one of the most used routing protocols in the wireless sensor networks applications. Its principle is based on the diffusion of interests by the base station. If a sensor node senses an event that responds to this request (Interest), it sends the sensed data to the node that transmitted the interest message.

Several variants of DD have been proposed [5, 6, 7, 8] in the literature to improve the original mechanism of this protocol and to better adapt it to the wireless sensor networks constraints.

The aim of our work is to implement a secure version of Directed Diffusion which will reduce the vulnerability of sensor networks and thus increase their lifetime. The remainder of this paper is organized as follows: In Section 2, we give an overview of the Directed Diffusion protocol. Section 3 describes some Attacks against routing protocols in WSNs. Section 4 gives a state of the art on the secure routing protocols in wireless sensor networks. The proposed solution securing Directed Diffusion to reduce energy consumption is presented in Section 5. The evaluation of this solution and the results interpretation are presented in Section 6 and the last section concludes the paper.

II. Directed Diffusion

Directed Diffusion [4] is a data centric protocols commonly used in wireless sensor networks. It consists of several elements: interests, gradients, data messages and reinforcements (positive and negative). An interest is a request, in which it specifies the desired data, sent by the base station (sink node) to the sensor nodes (Fig. 1(a)). A gradient is a response link to the neighbor from which the interest was received (Fig. 1(b)). Therefore, using the interest and gradients, routes are established between sensor nodes and sink node. Several routes can be set so that one of them is selected according to the rate. Data messages are events generated by one or more sensor nodes in response to requests sent by the base station.

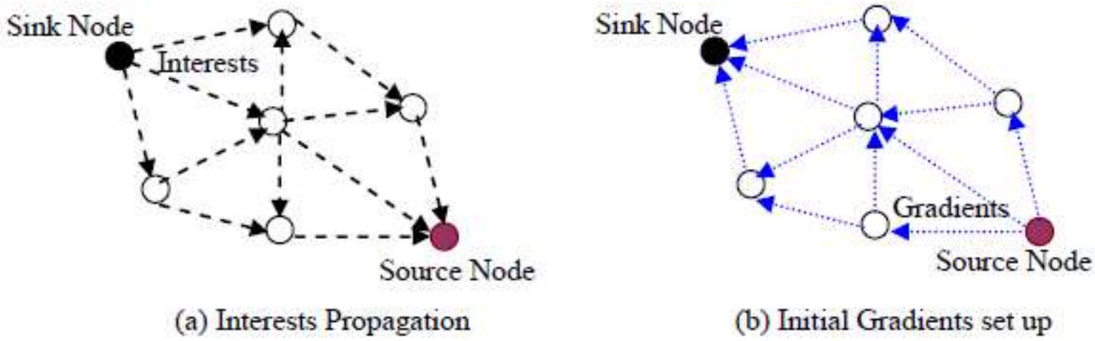


Fig. 1: Interest and gradient propagation

Interests and gradients are described by attribute-value model. When the sink requires a data, it broadcasts an interest containing several fields that depend on the application, such as: the type of required data, the rate of desired data and the time to live of the interest ... Interests initially specify a low rate of data flow, but once a base station starts receiving events it will reinforce one (or more) neighbor in order to request higher data rate. This process proceeds recursively until it reaches the nodes generating the events, causing them to generate events at a higher data rate. Alternatively, routes may be negatively reinforced as well.

Each node in the network maintains an interest cache which contains the information about the interest it received. Interest cache does not have information about the base station but the one-hop neighbor from which it received the interest. There are several fields in the interest cache as a time stamp field indicating the time stamp of the last event received. The interest cache also contains several gradient fields, up to one per neighbor. Each gradient contains the data rate field which specifies the data rate requested by the corresponding neighbor and also maintains a duration field.

When an interest reaches targeted sources, the sensors begin data collection. Then, the sensor node searches in its interest cache for a matching interest entry. If a matching interest is found then the node will look at the data rate parameter for all the gradients and forward the data at the rate specified. It will initially be slower for all gradients. So, all the neighbors receive a copy of the event. The source node unicasts the events, to all the neighbors for which it has a gradient. If the data rates of downstream nodes are different, then the source node sends the events to the highest data rate neighbor. The node which receives the events from the source, attempts to find a matching entry in its interest cache. If a match does not exist then the data message is deleted. Nodes of the sensor network may also send positive or negative reinforcement that increase or decrease the rate on a given path.

When the data message reaches the base station, this base station reinforces positively one particular neighbor, and that neighbor, reinforces one of its upstream neighbors. The reinforcement continues till the message reaches the source node (Fig. 2 (a)). The data message will be sent through this reinforced route (Fig. 2(b)). A base station can also send a negative reinforcement to remove unnecessary routes between the source node and the base station (Fig. 2(c)).

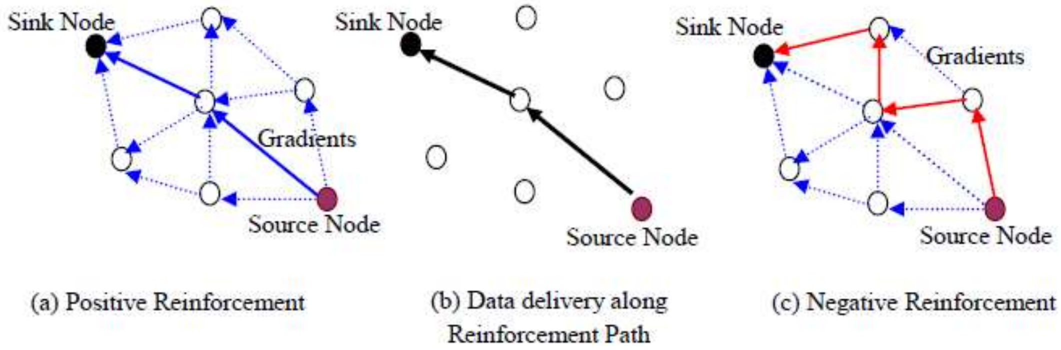

Sink Node
Gradients
Source Node
(a) Positive Reinforcement
Sink Node
Source Node
(b) Data delivery along Reinforcement Path
Sink Node
Gradients
Source Node
(c) Negative Reinforcement

Fig. 2: Reinforcement and data delivery

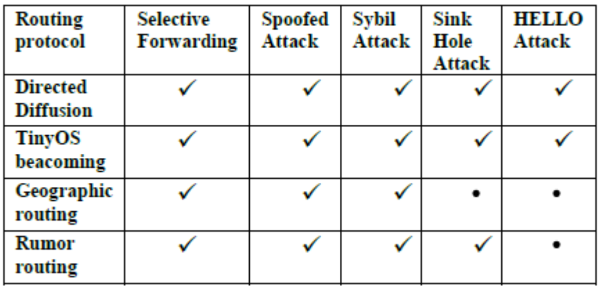
III. Attacks against Routing Protocols in WSN

In this section, we present some types of attacks against the WSNs [9, 10, 11], particularly those on the network layer. In the literature, several dangerous attacks on this layer are identified [12]. Most of them fall into one of the following categories:

- Routing loop: An attacker injects malicious routing information that causes other nodes to form a routing loop. Packets injected into this loop (both by legitimate and malicious nodes) are then sent in a circle, wasting precious communication and battery resources.
- General Denial-of-Service (DoS) attacks: By injecting malicious information or altering legitimate routing setup messages, an attacker can prevent the routing protocol from functioning correctly. For example, an attacker can forge messages to convince legitimate nodes to route packets in away from the correct destination. Wood and Stankovic [13] give taxonomy for DoS attacks against sensor networks.
- Sybil attack: A malicious node creates multiple fake identities to perform attacks [14]. In geographic routing protocols, fake identities can claim to be at multiple locations.
- Black hole attack: A malicious node advertises a short distance to all destinations, attracting traffic meant for those destinations. The attacker can selectively forward messages (although it may be difficult for them to leave the black hole).
- Sink holes: In a sinkhole attack [15], the adversary manipulates the neighboring nodes to attract nearly all the traffic from a particular area through a compromised node and create a sink hole. This malicious sink can now, not only tamper with the transmitted data but can also drop some vital data and lead to other attacks like selective forwarding. Low-cost routes may be erroneously flooded to lure the traffic [16].
- Wormhole attack: The wormhole attack [15] is a critical attack, where the attacker receives messages by making a tunnel and a low-latency link in one part of the network and replays them in a different part. An adversary could convince nodes which would normally be multiple hops from a sink that they are only one or two hops away via the wormhole. This would not only make some confusion in the routing mechanisms but would also create a sinkhole since the adversary on the other side of the wormhole can pretend to have a high quality route to the sink, potentially drawing all traffic in the surrounding area.
- Replication attack: An adversary may compromise a single legitimate node and insert copies throughout the network, increasing its presence in the network and thus allowing it to influence and subvert the network's performance.
- Selective forwarding: In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further.
- Flooding: A flooding attack overwhelms a victim's limited resources, whether memory, energy, or bandwidth. In a homogeneous network, an adversary node may have the same resource limitations as a victim, making an attack relatively expensive to mount. However, if an attacker possesses a more powerful device, such as a base station or laptop, the cost of the flooding attack relative to the result is much lower.
- HELLO flooding attack: Slightly different from conventional flooding, a HELLO flood is a single broadcast by a powerful adversary to many members of the WSN, announcing false neighbor status [15]. Many protocols use the exchange of HELLO packets to establish local neighborhood tables. The result of a HELLO flood is that every node thinks the attacker is within one-hop radio communication range and sends to this attacker the data packets. One possible solution to this attack is to use the authentication mechanism by a tiers sensor node [17].

Sadeghi [12] summarized the possible attacks on a set of routing protocols in wireless sensor networks as shown in table1. For example, geographic routing protocol suffers from three attacks: selective forwarding, spoofed attack and sybil attack but Directed Diffusion protocol suffers from all the attacks listed in this table.

Table 1: Attacks on routing protocols in Wireless Sensor Networks



Routing protocol	Selective Forwarding	Spoofed Attack	Sybil Attack	Sink Hole Attack	HELLO Attack
Directed Diffusion	✓	✓	✓	✓	✓
TinyOS beacoming	✓	✓	✓	✓	✓
Geographic routing	✓	✓	✓	•	•
Rumor routing	✓	✓	✓	✓	•

IV. Secure Sensor Network Routing Protocol

Many routing protocols have been specifically designed for WSNs [2, 3, 4]. But few of them take into consideration the vulnerabilities and the attacks against these networks [9, 10, 11, 12]. So, routing protocols should be resistant to these attacks. Security is very important for many applications in sensor networks and even critical for some others such as military target tracking and surveillance, natural disaster relief, biomedical health monitoring, environment exploration and agricultural industry. Below, we give some solutions presented in the literature to secure routing in wireless sensor network.

In [18] authors present Secure Implicit Geographic Forwarding (SIGF) routing protocol, a family of configurable secure routing protocols. As a preventive measure, this protocol chooses next hop dynamically and non-deterministically rather than maintaining routing tables. Deng et al [19] present an Intrusion-tolerant routing protocol for WSNs (INSENS). INSENS does not rely on detecting intrusions, but uses multipath technique in order to make the network resilient to attacks. The idea of INSENS is that an intruder may compromise a small number of nodes in the networks, but the damage is limited and does not spread in the network. Yin and Madria [20] proposed a hierarchical secure routing protocol against black hole attack (HSRBH). This protocol is the family of hierarchical routing protocols which applies MAC (Message Authentication Code) for integrity of the packets and Symmetric cryptography for discover a safe route against black hole attack. Zhang et al [21] proposed a Secure Routing Protocol for Cluster-Based Wireless Sensor Networks using Group Key Management (RLEACH). This protocol which is a family of cluster-based protocol can be thought as security extension of LEACH. This protocol is resistance against the different attacks such as selective forwarding, Sybil and hello flood attack. In [22, 23] a secure extension for the Directed Diffusion protocol is proposed. Authors in [22] derive an extension of Logical Key Hierarchy (LKH) and merge this extension with Directed Diffusion. The resulting protocol, LKHW combines the advantages of both LKH and Directed Diffusion. In [24] authors give a simple scheme to securely diffuse data. They considered the limited CPU processing capability, for witch they use an efficient one-way chain and do not use asymmetric cryptographic operations in this protocol. DAWWSEN (Defence mechanism Against Wormhole attacks in Wireless Sensor Networks) was introduced by Kaissi and al [23]. They presented a defence mechanism against wormhole attacks in wireless sensor networks. Specifically, a simple routing tree protocol is proposed and shown to be effective in defending against wormhole attacks.

V. The Proposed Solution to Secure Directed Diffusion

Directed Diffusion is a very popular routing protocol in wireless sensor networks. Unfortunately, it suffers from several vulnerabilities and attacks as shown in table 1.

Among the main objectives of attacks on routing protocols in sensor networks we notice the depletion of scarce energy resource. Energy is the major constraint of wireless sensor capabilities because once sensor nodes are deployed; they cannot be easily replaced or recharged. Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. For this, we are motivated to propose a secure version of Directed Diffusion to extend the network lifetime.

Securing this protocol requires to provide the basic security services such as authentication, data integrity, freshness of messages and confidentiality [10].

Any security processes need encryption keys. In our work, to secure Directed Diffusion, we use LEAP [24], a key management protocol in sensor networks. The choice of this protocol is motivated by the fact that it allows unicast and broadcast authentication and it is flexible in terms of energy consumption.

LEAP protocol uses four different keys to provide security in the network. But in our work, to secure Direcetd Diffusion and regarding to the different types of transmissions in this protocol, we use three types of keys. These keys are: the individual key of a node u (IKu), which is used to secure communication between a node and the base station, the pair-wise key (Kpair) to secure communication between a node and one of its neighbors and finally the global key (BK), all the nodes in the sensor network share this key with the base station. The base station uses global key to encrypt the interest message and all the nodes in the network uses this key to decrypt the announcements from the base station. The nodes store the interest information in their interest cache and then encrypt the message using the global key to further broadcasting it. The communication cost is reduced by using this key. The forth key of LEAP is the cluster key, but in our work, we do not need this key as in Directed Diffusion protocol, all the communications are between one hop neighbors.

The global and individual keys are loaded into all the nodes in the network before deployment. However, the pair-wise key is established after the network deployment. Once all keys are established, the base station can broadcast the interests to ask the sensor nodes about the required data.

To ensure the authentication, the MAC (Message Authentication Code) can be calculated on the node identifier (Id). To ensure the data integrity, the MAC can be calculated on the data. In this work, to ensure both authentication and integrity of data to transmit to the sink node, we calculate the MAC on the identifier and the data at the same time, we note this DATA (DATA = Id + data). In the case of an interest packet which is broadcasted to all the neighbors we calculate the MAC by using the global key (MAC (DATA, BK)). But if the packet is a data packet or a reinforcement packet which is sent to one of the neighboring nodes, we calculate the MAC by using the pair-wise key (MAC (DATA, Kpair)).

To ensure confidentiality, we have encrypted the data using the pair-wise key and the RC5 algorithm [25]. This algorithm is chosen for its low power consumption.

The data freshness is ensured by integrating a TimeStamp field in each packet sent across the network.

A packet is considered fresh by the receiving node, if the difference between the receipt time of the packet and its send time (TimeStamp) is less than a certain value.

VI. Simulation and Results Interpretation

In this section, we evaluate the performance of our proposed solution by doing a set of simulations under Jsim simulator [26].

We compare the performance of our solution (secure Directed Diffusion) with the original version of Directed Diffusion protocol. Our experimental model is established on 50 nodes, randomly dispersed in an area of 600x600 m2. We assume that all nodes are not mobile throughout the simulation period and are homogeneous; i.e. all nodes have the same capacity in terms of energy and memory unless the base station is assumed to have a greater capacity and can not be compromised.

The implemented attack consists on rebroadcasting the interest packet by the malicious node; Interests received by the malicious node are sent in the network several times, wasting precious communication and battery resources. Consequently, the network lifetime is reduced.

The performance metric considered for the comparison of these two protocols is energy. We perform two sets of simulations. In the first case, we compare Directed Diffusion and secure Directed Diffusion in the absence of attacks. In the second case, we perform the same comparisons in the presence of attacks.

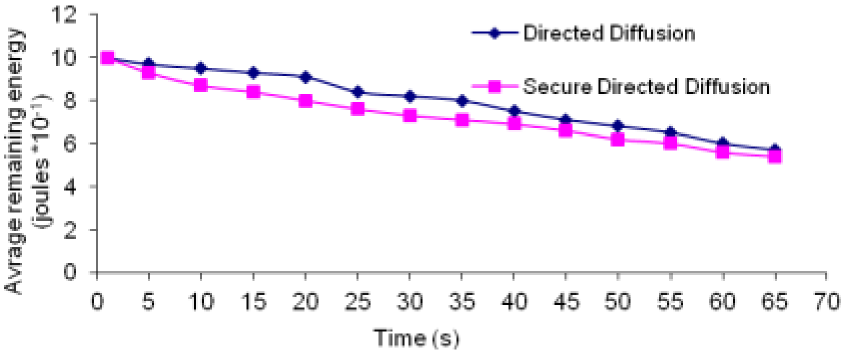


Fig. 3: Average remaining energy vs. Time in absence of attacks

Fig. 3 shows the simulation results for Directed Diffusion and secure Directed Diffusion in the absence of attacks. These results show that the variation of the average remaining energy versus time is almost the same for both protocols. We note that despite the additional phase of secure Directed Diffusion which consists of keys establishment, the amount of energy consumed by the secure Directed Diffusion is insignificant compared to that consumed by Directed Diffusion. So our solution is not disadvantageous in terms of energy consumption.

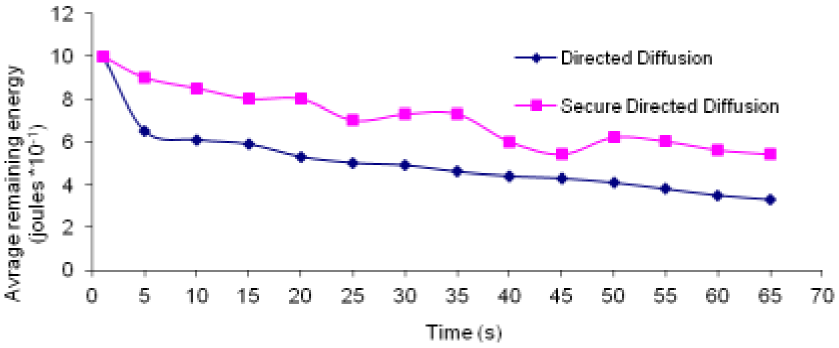


Fig. 4: Average remaining energy vs. Time in presence of attacks

Fig. 4 shows the results obtained by simulating Directed Diffusion and secure Directed Diffusion in the presence of attacks. We notice that Directed Diffusion is very vulnerable to attacks. Thus, the attacks can significantly reduce the lifetime of the sensor network. Each interest packet received by the attacker is retransmitted several times to all neighbors' nodes, which consumes a lot of energy because the transmission module is the module consuming the most energy on the node. However, the secure Directed Diffusion presents better results. This shows that our solution protects the network of premature death by detecting and preventing attacks.

VII. Conclusion

Energy and security are vital to the acceptance and use of wireless sensor networks for many applications in our daily life. However, the most current researches do not considers simultaneously energy and security constraints in WSNs. In view of this need, we have proposed a new solution which deals with both energy and security in routing protocols. Specially, we have secured Directed Diffusion protocol in order to reduce the power consumption of nodes, so the lifetime of the network will be extended. The obtained results show that secure Directed Diffusion outperforms the original version of Directed Diffusion in terms of energy in presence of the attacks.

References

[1] S. K. Singh, M P. Singh, and D. K. Singh. Routing Protocols in Wireless Sensor Networks – A Survey [J] Computer Science & Engineering Survey (IJCSES), Nov 2010, 1(2): 63-83.

[2] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless micro sensor networks[C]. IEEE Proc. Hawaii Int',l. Conf. System. Sciences, Jan 2000.1 -10.

[3] J.Kulik, W. R. Heinzelman, and H. Balak-rishnan. Negotiation- based protocols for disseminating information in wireless sensor networks [J]. Wireless Networks, 2002, 8(2/3):169-185.

[4] C. Intanagonwiwat, R. Govindan and D. Estrin. Directed Diffusion: a scalable and robust communication paradigm for sensor networks[C]. Boston, Massachusetts, USA. ACM. MOBICOM, 2000.56-67

[5] M. Chen, T. Kwon, and Y. Choi. Energy-efficient differentiated directed diffusion (eddd) for real-time traffic in wireless sensor networks [J]. Elsevier Computer Communications Journal, Special Issue on Dependable Wireless Sensor Networks, Jan 2006

[6] K. E. Kannnammal, and T. Purusothaman. New Interest Propagation in Directed Diffusion Protocol for Mobile Sensor Networks [J]. European Journal of Scientific Research, 2012, 68(1): 36-42

[7] V. R. Kumar, J. Thomas, and A. Abraham. Secure Directed Diffusion Routing Protocol for Sensor Networks using the LEAP Protocol [M]. NATO Security through Science Series -D: Information and Communication Security, Vol. 6, pp. 183-203, 2006

[8] X. Wang, L. Yang, and K. Chen. SDD: Secure distributed diffusion protocol for sensor networks [A]. Proceedings of the 1st European Workshop on Security in Ad Hoc and Sensor Networks, LNCS 3313, 2005. 205-214.

[9] G. Padmavathi, and D. Shanmugapriya. A survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks [J]. International Journal of Computer Science and Information Security (IJCSIS), 2009, 4(1 & 2):1-9.

[10] M. K. Jain. Wireless Sensor Networks: Security Issues and Challenges [J]. International Journal of Computer and Information Technology (IJCIT), 2011, 2(1): 62-67.

[11] S. K. Singh, M. P. Singh, and D. K. Singh. A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks [J]. International Journal of Computer trends and Technology, May to Jun, Issue 2011.

[12] M. Sadeghi, F. Khosravi, K. Atefi, and M. Barati. Security Analysis of Routing Protocols in Wireless Sensor Networks [J]. International Journal of Computer science Issues (IJCSI), Jan 2012, Vol. 9, Issue 1, N °3: 465-472

[13] A. D. Wood, and J. A. Stankovic. A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks [M]. Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005.

[14] Newso James, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks: analysis & defenses[C]. In Proceedings of the 3rd international symposium on Information processing in sensor networks, IPSN '04, New York, NY, USA, 2004. 259-268.

[15] C. Karlof, and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures [J]. Ad Hoc Networks, 2003, 1(2-3):293-315.

[16] A.D. Wood, and J.A. Stankovic. Denial of service in sensor networks [J]. Computer, Oct 2002, 35(10):54-62.

[17] D.R. Raymond, and S.F. Midki. Denial-of-service in wireless sensor networks: Attacks and defenses [J]. Pervasive Computing, IEEE, Jan.-Mar 2008. 7(1): 74-81.

[18] A. D. Wood, L. Fang, J. A. Stankovic, and T. He. SIGF: A family of configurable secure routing protocols for wireless sensor networks [A]. In Proceedings of the 4th ACM Workshop Security of Ad hoc Sensor Networks, 2006. 35-48.

[19] J. Deng, R. Han, and S. Mishra. INSENS: Intrusion-tolerant routing for wireless sensor networks [J]. Computer Communications, 2006, 29(2): 216-230.

[20] M. Senjay, and Y. Jian. SeRWA: A secure routing protocol against wormhole attacks [J]. Ad Hoc Networks, 2009, 7(6):1051-1063.

[21] Z. Kun. A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management[C]. International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08), Oct 2008. 12-14.

[22] 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 [A]. Proceedings of International Conf. Parallel Processing Workshops, 2003.397-406.

[23] R.El Kaissi, A. Kayssi, A. Chehab, and Z. Dawy. DAWWSEN: A Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks[C]. Proceedings of the Second International Conference on innovations in information Technology, UAE, Sep 2005.

[24] S. Zhu. LEAP: efficient security mechanisms for large-scale distributed sensor networks [A]. Proceedings. of the 2nd ACM International workshop on wireless sensor networks and applications, 2003. 62-72.

[25] R. Rivest. The rc5 encryption algorithm [A]. Proceedings of the 2nd Workshop on Fast Software Encryption (LNCS 1008), 1995. 86-96.

[26] J-Sim, http://www.j-sim.org/.

Authors' Profiles

Belkadi Malika: She received her engineering degree on computer science in 1998 and his PHD in 2011. Actually, is an assistant Professor at computer science department of Mouloud Mammeri University, Tizi Ouzou, Algeria. She is also a research member at the Laboratory (LARI) of the computer science department. Her areas of interest include mobile networks (Cellular, Ad hoc and sensors networks), embedded systems and computer architecture.

Aoudjit Rachida: She received her engineering degree on computer science in 1998 and his PHD in 2011. Actually, is an assistant Professor at computer science department, at the Faculty of Electrical Engineering and Computer Science, University of Tizi Ouzou. She is also a research member at the Laboratory (LARI) of the computer science department. Her areas of interest include mobile networks (Cellular, Ad hoc and sensors networks), embedded systems and computer architecture.

Daoui Mehammed: He received his engineering degree on computer science in 1997 and his PHD in 2009. Actually, is an assistant Professor at computer science department of Mouloud Mammeri University, Tizi Ouzou, Algeria. He is a research member at the Laboratory (LARI) of the Computer Science Department. His areas of interest include mobile networks (Cellular, Ad hoc and sensors networks), embedded systems and computer architecture.

Lalam Mustapha: He received the Master's degree in computer architecture from the High School of Computer Science, Algiers, Algeria, in 1980 and the PHD. degree in computer science from the University of Toulouse, France, in 1990. He joined the University of Tizi Ouzou, Algeria in 1993, where he is now Professor in the Computer Science Department at the University of Tizi Ouzou. He has been involved in research and development of computer architecture, distributed systems and mobility management for wireless mobile computing and communications.

How to cite this paper: Malika BELKADI, Rachida AOUDJIT, Mehammed DAOUI, Mustapha LALAM,"Energy-efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks", International Journal of Information Technology and Computer Science(IJITCS), vol.6, no.1, pp.50-56, 2014. DOI: 10.5815/ijitcs.2014.01.06