International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

A Short Survey on Secure Routing Protocols in Hierarchical Cluster-Based Wireless Sensor Networks

F.MEZRAG[1], M.BENMOHAMMED[2], B.BOUDERAH[3]

[1,3] Department of Computer Science, University of M'Sila, Algeria
[2] Department of Computer Science, University of Constantine 2, Algeria

---

Abstract -

The hierarchical routing protocols based on clusters rely fundamentally on their CHs for data aggregation and routing. They are vulnerable to several attacks, such as Hello flood, Selective forwarding, replay, etc; attacks involving CH are the most damaging. If a malicious node managed to become a CH, it can launch attacks to disrupt the network operation. Note that, the malicious node can choose to not attack the CH, and also try to inject erroneous information into the network. There is various secured routing protocol to resist the attacks.

Key Words: *Wireless Sensor Networks, Secure Routing Protocols, Cluster Head*

1. INTODUCTION

The wireless sensor network (WSN) is a collection of sensor nodes (small appliances) deployed at random or deterministic manner in an area of interest. These nodes can exchange data between them without using a preexisting and fixed network infrastructure or centralized administration.

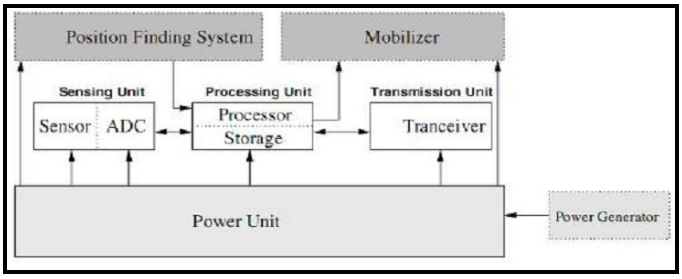

Fig -1: Physical structure of a sensor node

The physical structure of a sensor node is shown in Fig-1. Each network node communicates directly with other nodes that are within its radio Proteus (communication range). The communication with the remote node or out of radio range is done through other nodes that route data to destination. This process is done through the routing protocol. The routing is a fundamental function in each network, it is based on a multi-hop communication and wireless sensor networks are not exceptional. Several routing protocols have been proposed for WSNs. They are generally classified into two categories [1]: Network structure and Protocol operation. Network Structure is further classified into Flat, Hierarchical and Location based routing. Protocol Operation is further classified into Negotiation, Multi-path, Query, QoS and Coherent based routing. Cluster-based hierarchical routing protocol is an effective way to reduce the total energy consumption of the wireless sensor network. The idea is to form groups (clusters) of sensor nodes and use CHs (Cluster-Heads) elected as routers. Each CH collects data from all the sensor nodes belonging to their cluster, aggregates the data collected and transmitted directly to the base station (BS). The data aggregation and processing in CH significantly reduces the total number of messages sent to the BS. Generally, the problems of security in hierarchical routing protocols do not have a great deal of attention, since most of these protocols have been developed for the purpose the efficient routing of information; however the security aspect has been neglected. Indeed, they are vulnerable to attacks threatening the reliability of data traffic. The rest of the paper is organized as follow: In Section 2, we are exhibiting major hierarchical routing protocols. In section 3, we present an overview of security requirements. Section 4 describes the classification of attacks and attacks that are carried out against routing. Section 5 exhibits a set of secure hierarchical routing protocols. Security analysis being made in section 6.

2. HIERARCHICAL ROUTING PROTOCOLS

In this section, we will try to present the major hierarchical routing protocols in the literature. LEACH [2] was a protocol for hierarchical routing based on cluster proposed for homogeneous sensor networks. Its operation is divided into several rounds. In each round, we find two phases: set-up phase and steady-state phase. In the first phase, the CHs are selected and clusters are formed where the election process is triggered to choose future CHs. Each node n generates a random number x, ($0 < x < 1$). If x is less than a threshold value T then the node n acts as CH in the current round, otherwise it is a member of the cluster. In the second phase, data collected by sensor nodes are communicated to the base station. CHs are dynamic, they change randomly with time to balance the energy dissipation by the nodes. TL-LEACH [3] is an

extension of the LEACH algorithm, it uses two levels of CHs (primary and secondary) instead of a single level. In this Protocol, the primary CH in each cluster communicates with the CHs secondary, and these last communicate in their turn with the sensor nodes in their sub-group (Sub-Cluster). Data fusion can also be performed as in LEACH. The set-up phase for TL-LEACH is to form clusters and to select the primary and secondary CHs using the same mechanism as LEACH. TEEN [4] and APTEEN [5] have been proposed for critical applications in terms of time. In TEEN, nodes capture continuously, but data transmission is not done frequently. This is a protocol designed to be sensitive to sudden changes in certain attributes captured in WSN (e.g. temperature). The majority of TEEN behavior is similar to the LEACH Protocol. However, some differences exist. After the formation of clusters, each CH transmits two thresholds to its members instead of transmitting a TDMA (Time Division Multiple Access) schedule. These two thresholds, noted HT (Hard Threshold) and ST (Soft Threshold) for the detected attribute. HT: Determines the minimum value beyond which members are likely to transmit their data reports. ST: Specifies the minimal change requiring the node to send new data report. When the sensed value exceeds HT, it must send the report data to CH. It does not transmit a new report if the difference between the current value and the previous value exceeds ST. TEEN allows to build a reactive behaviour, which allows to minimize the number of messages and to save energy. However, the main drawback of this protocol is that if the HT and ST thresholds are not achieved, the nodes are not possible to communicate, and no data will be transmitted to the user and the base station does not know the nodes that have exhausted their energy. To remedy this situation, the authors proposed an extension of TEEN called APTEEN which allows to find a compromise between proactive hierarchical protocols (as LEACH) and reactive hierarchical protocols (as TEEN). APTEEN allows sensor nodes to perform the same threshold mechanism of the protocol TEEN, and in the case where the node does not transmit data for a period exceeding time TC, it should perform a data transfer to CH during its slot TDMA. PEGASIS [6] is an improved version of LEACH. The basic idea is to form a chain between the nodes so that each node communicates only with two nodes directly connected with this chain. This allows to minimize the energy dissipation by the sensor nodes. At each round, a single node (leader) of the chain is selected for transmission to the BS. The data collected are transmitted from one node to another which aggregates them until they arrive at a node (leader) that transmits them to the BS. PEGASIS presents an excessive delay of remote nodes in the chain. Thus PEGASIS does not guarantee delivery of data to BS at each round since a node can fail in its role of leader. Hierarchical-PEGASIS [7] is an improved extension of PEGASIS Protocol whose purpose is to reduce the delays of transmission of the data to the BS.

3. Basic security requirements

The security requirements in a sensor network should protect the information provided on the network and resources against attacks and misbehavior nodes. The most important security requirements are:

- *Confidentiality*: The security mechanism should ensure that no message in the network is understood by anyone except intended recipient.
- *Integrity*: ensuring that messages are not altered in transit in the network.
- *Authentication*: The ability to verify the validity of the identity of the issuer.
- *Freshness*: involving the messages are recent and current.
- *Availability*: ensures that services a network should always be available even in the presence of internal or external attacks.

4. ATTACKS AGAINST WSN

Attacks against WSN can be classified into the following categories:[8, 9, 10]

4.1 External attacks VS. Internal attacks

The external attack is launched by a node that does not belong to the network, or that doesn't have permission to access. The internal attack is launched by a malicious internal node. This latter is a type of the most severe threat that can disrupt the functioning of sensor networks, since defence strategies generally aim to combat external attacks.

4.2 Passive attacks VS. Active attacks

The objective of the passive attack is to obtain information without being detected. Usually, the attacker is limited to listening to the traffic exchanged. It collects a large volume of data and performs data analysis to extract secret information or knowledge of important nodes in the network (cluster-head). This extracted information can then serve the attacker for malicious purposes. Contrariwise, in active attacks, attacker alters, misroutes, replays or blocks arriving messages.

4.3 Physical attacks VS. Remote

In a physical attack an adversary physically accesses to the sensor node which should be injured by the falsification or destruction of the sensor hardware. On the other hand, remote attack is implemented from a distance, for example, by emitting a high energy signal to interrupt the communication.

4.4 Mote-class attacks VS. Laptop-class attacks

The attack mote-class occurs by a sensor node. In other words, the device of attack is of the same type of material as the sensor nodes that should be attacked. On the other hand, in the laptop-class attack, the adversary uses a

device that is greater than the sensor nodes that should be attacked in terms of computing power and transmission power.

4.5 Attacks against routing

Routing protocols in WSN suffer from many attacks [10] that are:

-*Spoofed, altered and replayed routing information:* It allows to target information exchanged between sensor nodes [10]. An attacker may inject previous exchanges intercepted by it, or false data in the network to confuse the sensor nodes. A malicious node may also modify data received before sending them to the final destination.
-*Selective forwarding*: The attacker can insert or compromise sensor nodes in the network so that these malicious nodes refuse to forward some packets from neighboring nodes. The choice of packets is based on certain criteria (content of the packets, source address of the transmitter) or in a random manner.

-*Sinkhole and Wormhole:* In a sinkhole attack, the malicious node tries to attract to him the most possible traffic to control much of the data circulating in the network to prevent the BS to get complete and correct data. A wormhole attack creates a strong link connection (tunnel) between two malicious nodes used by the adversary for injection, modification and data retransmission.

-*Sybil attack*: a malicious node collects multiple identities in the network. Either by manufacturing or by theft of the identity of legitimates nodes. This attack can degrade the effectiveness of several features such as the distribution of data, aiming to change the data integrity and routing mechanisms.

- *Hello flood*: an attacker tries to send a flood of such packets (Hello) in order to consume the energy of sensor nodes and to prevent their messages to be exchanged.

5. SECURE HIERARCHICAL ROUTING PROTOCOLS

The existing hierarchical routing protocols in the literature are the assumption of an ideal environment in which the operation of the network is not subject to malicious attacks. Different techniques have been proposed to secure this type of routing protocols. In this section, we give an overview of a set of secure hierarchical routing protocols.

SLEACH [11]: This protocol is the first secure version of LEACH. It uses the protocol SPINS [12] (Security Protocol for Sensor Network) and MAC (Message Authentication Code) to provide protection against attacks: selective forwarding, sinkhole and HELLO flooding. SLEACH prevents an intruder to become CH or send falsified data to CH. But it doesn't guarantee confidentiality and availability (insider adversary can decrease networks throughput by disrupting the time slot schedule of a cluster).

SecLEACH [13]: Is a modified version of LEACH who has the ability to resist to several attacks such as selective forwarding, Sybil and HELLO flooding by using a probabilistic scheme and μTESLA[12]. Sec-LEACH prevents unauthorized nodes become CH, it also provides authentication, integrity, confidentiality and freshness of messages.

SS-LEACH [14]: Is another secure version of LEACH; its main goal is to offer security while being energy efficient. For that, it defines stochastic multipaths cluster heads chains to communicate with the base station, which prolongs better the network lifetime. To ensure security, it employs key pre-distribution and self localization techniques. SS-LEACH prevents attacks such selective forwarding, hello flooding and Sybil attacks, but it controls neither data integrity nor freshness.

RLEACH [15]: Is considered as secure extension of LEACH. The developers of this Protocol have tried to apply an improved version of key management scheme based on the RPK [16] (Random Pairwise Key managent) on LEACH. The basic version of RPK is not adaptable to LEACH since it does not guarantee that all adjacent nodes have shared key. RLEACH has the ability to resist to several attacks such as selective forwarding, sybil and hello flooding.

AC [17]: is considered a secure extension of LEACH, which is based on asymmetrical cryptography. It ensures the three security services: authentication, integrity and confidentiality partial (CH-SB). It is not expensive in terms of memory space (3 keys only stored in each node). This protocol eliminates the reference to the base station and uses asymmetric keys allowing to scale more easily. However, this protocol has the disadvantage that the authors mainly focus on how to secure the steady-state phase, while the set-up phase remains without security, it explains that malicious nodes can participate during the formation of clusters and CH become. Another negative of this protocol is that the operation of public key encryption, generation and verification of digital signatures is costly in terms of computing time and energy consumption.

Table-1: secure hierarchical routing protocols comparison based on security requirements.

security requirements	Secure Hierarchical Routing Protocol				
	SLEACH	SecLEACH	SS-LEACH	RLEACH	AC
Confidentiality		x	x		x
Integrity	x	x		x	x
Authenticity	x	x	x	x	x
Freshness	x	x			

Table-2: Resistance of routing attacks for secure hierarchical routing protocols

Routing Attacks	Secure Hierarchical Routing Protocol				
	SLEACH	SecLEACH	SS-LEACH	RLEACH	AC
Alter	x	x	x	x	x
Replay	x	x	x	x	
Selective Forwarding	x	x	x	x	
Hello Flood	x	x	x	x	
Sybil		x	x	x	
Sinkhole	x			x	
Wormhole					

6. SECURITY ANALYSIS

Security requirements for several routing protocols are summarized in Table 1. We observe that SecLEACH address all the listed security requirements, thus it is more secure than rest of the protocols if the security requirements is taken as criteria. According to the security requirements, selected protocols classification show that authentication and integrity are the most satisfied. Considering the resistance against the routing attacks, Table 2 shows that RLEACH, SLEACH, SecLEACH and SS-LEACH are more resistant to routing attacks than rest of the secure protocols.

7. CONCLUSION

The hierarchical routing protocols in sensor networks are specified without any security measures (LEACH, TEEN, and PEGASIS). However, the security services are identified as essential to ensure widespread deployment of these networks. In this paper, we have focused on the security of hierarchical routing protocol based on clustering for wireless sensor networks, we addressed and analysed some secure cluster based routing protocols. We also presented a comparative study based upon various criteria.

REFERENCES

[1] J. N. Al-Karaki and A. E. Kamal. Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communication*, 11(6), December 2004.

[2] A. Chandrakasan W. Heinzelman and H. Balakrishnan. Energy-efficient communication protocol for wireless sensor networks. In *Proceedings of the IEEE Hawaii International Conference on System Sciences*, pages 3005–3014, January 2000.

[3] G. Morabito V. Loscr and S. Marano. A two-levels hierarchy for low-energy adaptative clustering hierarchy (tl-leach). In *Proceedind of VTC2005*, pages 1809–1813, Dallas (USA), September 2005.

[4] A. Manjeshwar and D. P. Agrawal. Teen: A protocol for enhanced efficiency in wireless sensor networks. In *Proceedings of the International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, 2001.

[5] A. Manjeshwar and D.P. Agarwal. Apteen: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In *the 16th International Parallel and Distributed Processing Symposium*, April 2002.

[6] S. Lindsey and C. S. Raghavendra. Pegasis : Power efficient gathering in sensor information systems. In *Proceedings of the IEEE Aerospace Conference*, volume 3, 2002.

[7] K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. *Ad hoc Networks*, 3(3):325 – 349, 2005.

[8] N. Badache D. Djenouri, L. Khelladi. A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications Surveys and Tutorials Journal*, pages 2–29, 2005.

[9] O. Alfandi A. Kellner and D. Hogrefe. A survey on measures for secure routing in wireless sensor networks. *International Journal of Sensor Networks and Data Communications*, 1:17, May 2012.

[10] C. Karlof and D. Wagner. Secure routing in sensor networks: attacks and countermeasures. *Ad Hoc Networks*, pages 293–315, May 2003.

[11] L. B. Oliveira E. Habib H. C. Wong A. C. Ferreira, M. A. Vilaa and A. A. Loureiro. On the security of cluster-based communication protocols for wireless sensor networks. In *Proceedings of 4th IEEE International Conference on Networking*, volume 3420, pages 449–458, 2005.

[12] V. Wen D. Cullar A. Perrig, R. Szewczyk and J. D. Tygar. Spins: Security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, 2002.

[13] M. A. Vilaa H. C. Wong M. Bern R. Dahab L. B. Oliveira, A. Ferreira and A. A. F. Loureiro. Secleach-on the security of clustered sensor networks. In *Signal Processing*, volume 87, pages 2882–2895, December 2007.

[14] Di Wu and Gang Hu. Research and improve on secure routing protocols in wireless sensor networks. In *4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008)*, pages 853–856, May 2008.

[15] C. Wang K. Zhang and C. Wang. A secure routing protocol for cluster-based wireless sensor networks using group key management. In *4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM08)*, pages 1–5, October 2008.

[16] A. Perrig H. Chan and D. Song. Random key predistribution schemes for sensor networks. In *IEEE Security and Privacy Symposim 2003*, pages 197–213, May 2003.

[17] R. Srinath. A. Vasudev Reddy. and R. Srinvasan. AC : Cluster Based Secure Routing Protocol for WSN.

IEEE, Third International Conference in Networking and Services (ICNS'07), 2007.

BIOGRAPHIES

Fares MEZRAG is currently a director of center of networks and systems of information and communication, University of M'Sila, Algeria. He received his Magister from University of Laghouat, Algeria in 2015. His area of interest is embedded systems, distributed computer systems, computer networks with WSN, security.

Prof.Dr.Mohamed BENMOHAMMED is Professor at University of Constantine 2 Algeria. He received his Doctorate in Automatic Generation of reprogrammable architectures in High Level Synthesis Environment from University of SBA, Algeria in 1997, and Full professor in 2005. His research interests are CAO-VLSI, High Level Synthesis, Controllers, ASIP, ASIC, DSP, RDP Formal verification, Simulation, Parallel Architectures, Networks. He is the author and co-author for several national and international publications in technical journals and conferences.

Prof. Dr. Brahim BOUDERAH is currently a Vice - Rector of Development, Forecasting and Orientation, University of M'Sila, Algeria. He received his Doctorate in Applied Mathematics from University of Setif, Algeria in 2001, and Full professor in 2007. His area of interest is Fluid Mechanics, Free Surface Flow Computation, Operational Research, Applied Mathematics, Optimisation in Air Traffic Network, Security with ADN's calculus, Bioinformatics and Image segmentation. He is the author and co-author for several national and international publications in technical journals and conferences.

