JWSN 2016, 3, 1-0013

Journal of Wireless Sensor Networks
ISSN: 2001-6417
www.wsn-journal.com

Article

Secure Clustering Protocols in Wireless Sensor Networks

Santar Pal Singh[1] , S. C. Sharma[1]

[1]Electronics and Computer Discipline, DPT, Indian Institute of Technology Roorkee-247667 (India)

spsingh78@gmail.com

Received: 11th August 2015 / Accepted: 11th December 2015/ Published: 21st January 2016

Abstract: Wireless sensor networks (WSNs) are poised of huge number of low-cost and tiny devices i.e. senor nodes which communicate over wireless media. Various WSN based projects produced fruitful and interesting results that greatly improves our life. Due to several limitations on the resources of sensor nodes, the networks exposed against different types of attacks. Hence, security in sensor networks is a prime issue and becomes hot topic for researchers. In this paper, we have been reported a detailed analysis on secure cluster-based routing protocols in WSNs. Finally, we propose a matrix which generalizes the work and suggest the protocol suitability for particular application.

Keywords: wireless sensor network; cluster-based routing; attacks; security; matrix

1. Introduction

Recent developments in wireless communication and low-cost sensor technology have enabled the emergence and evolution of wireless sensor networks (WSNs) as new paradigm of computer networking [1]. A wireless sensor network is poised of huge number of cheap and small sized sensor nodes enabled with sensing, processing and transmitting capabilities [2,3]. The wireless sensor networks were initially motivated by military applications but nowadays, WSNs are used in various civilian application areas like: monitoring, tracking, control, automation and healthcare applications. The collected data might be susceptible and pertinent to privacy, which cause security a key issue [4,5]. Unlike traditional networks, parameters such as open communication medium, restrictions on node's communication capabilities, and bandwidth discriminations constraints make sensor networks more vulnerable to attacks [6]. To extend network lifetime and lessen energy utilization, the clustering model for WSN was proposed [7]. A simple wireless sensor network is shown in figure 1.

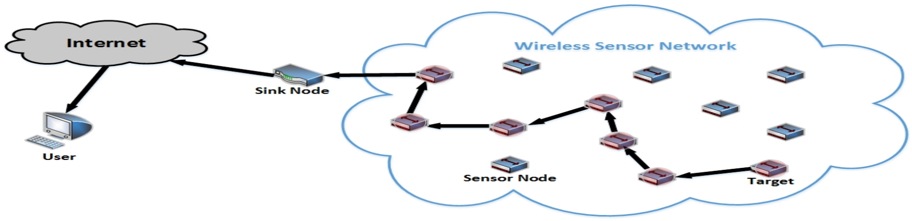

Figure 1. A simple wireless sensor network (Source:[8])

A clustering model for WSN is shown in figure 2. In the clustering model for wireless sensor networks, nodes energy is set aside by linking them in intra cluster communication and accomplishing data aggregation and data fusion. Each cluster has a leader node known as cluster head (CH) that is accountable for data collection among all nodes within the cluster and transfers the collective data to the base station (BS). The conventional security mechanisms are not suitable for WSNs as they are heavy and nodes are limited. Most of the schemes appraised the secure cluster-based routing protocols based on following processes only i.e. selection of cluster head and formation of cluster. While some schemes aims the protection of data transmission between CHs and BS. For any secure cluster-based routing protocols, set of criteria must be used for the effectiveness.

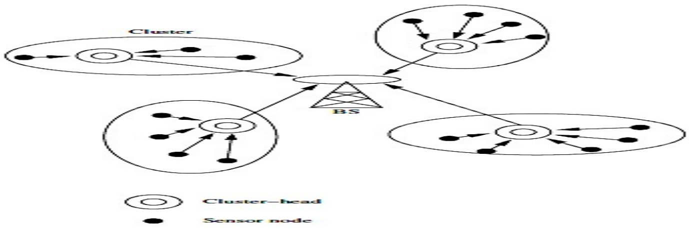

Figure 2. Clustered WSN (Source:[9])

These methods includes secure selection of cluster head, secure formation of cluster, secure aggregation of data, secure routing of data from CHs to BS, robustness against diverse type of attacks, efficient utilization of resources, and ability to deal with dynamic environment. Some schemes consider that all selected protocols that are explained are efficient and secure [10]. However, when different security mechanisms are used, less attention is paid on energy consumption. This is very important as deterministic and probabilistic strategies based schemes have diverse impacts on energy utilization. Hence, energy usage will directly affect performance of the network. The performance requirement study is also important because it is strictly bound to consume energy. The rest of the paper is organized as follows: routing in WSNs is presented in section 2. Section 3 briefly reviews the security issues in WSNs. Secure cluster-based routing protocols are discussed in section 4. The comparative security analysis is discussed in section 5. Finally, section 6 concludes the paper.

2. Routing in WSNs

In comparison to traditional networks, wireless sensor networks offer improved functionalities to monitor larger scaled and changing topology with limited power and computational capabilities. However, sensor nodes have several limitations in term of energy and bandwidth utilization. Such constraints pose several challenges to WSNs architecture and impose energy-awareness at protocol stack. Hence, at network layer, it is highly desirable to find out various methods for efficient discovery of rout and pass on the data from sensor nodes to base station to maximize the network lifetime. Routing is the process of selecting best path in the network. Routing protocols [11,12] in WSNs are responsible for discovering and maintaining energy efficient routes, in order to make communication reliable and efficient. Figure 3 shows the classification of WSN routing protocols.

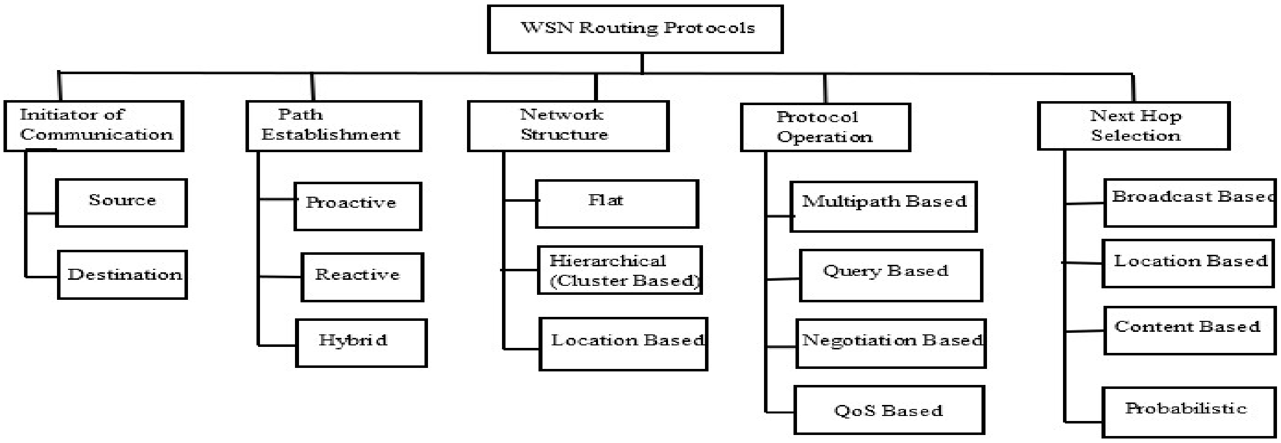

Figure 3. Taxonomy of WSN routing protocols (Source:[13])

Wireless sensor network's routing protocols are classified on the basis of initiation of communication, establishment of paths, structure of network, selection on next hop, and protocol operation. On the basis of next hop selection for packet forwarding, routing protocols can be categorized into following categories: broadcast based, location based, content based, and probabilistic. On the basis of literature review on network structure based routing schemes, WSNs routing protocols can be classified into following categories: flat routing, hierarchical or cluster based routing and location based routing. Flat routing uses tremendous equal sensors which works together to sense the phenomena. In hierarchical routing, sensor node pass on the data to a node(s) in higher hierarchy than the sender, this node is called aggregator, and then be forwarded to base. Location based protocols selects the next hop on the basis of the position of neighbour and destination.

3. Security Issues in WSNs

Security is vital in WSNs and attaining security objectives is a tough task as resources constrained nature of senor network. Many of the traditional security techniques for WSNs are not desirable due to resource limitations in these networks. Brief discussion on various security issues is stated in this section.

3.1. *Basic Security Requirements in WSNs*

In order to attain security in sensor networks certain security requirements must be provided. System must fulfil some of these requirements depending on applications [14,15]. The basic security requirements in sensor networks are shown in figure 4.

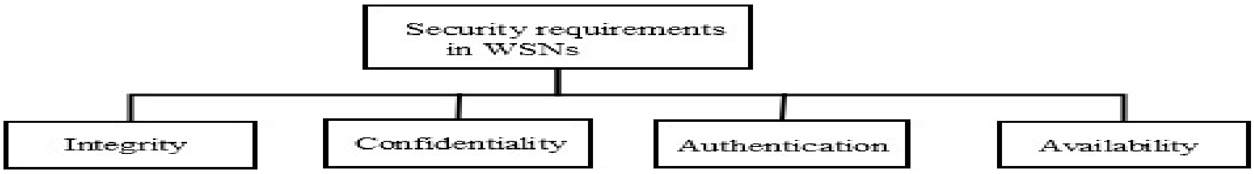

Figure 4. Basic security requirements in WSNs

The basic security requirements can be stated as follows [16]:

- ***Integrity:*** Transmitted data should not be altered in communication, and certain procedure must be followed to make sure that illegal party cannot be changed the data.
- ***Confidentiality:*** Confidentiality forbid delicate information from delivering to the wrong one, while ensures that right one can get it actually.
- ***Authentication:*** Authentication is the capability to recognize the reliability of the origin of message.
- ***Availability:*** Availability necessitates the data availability to legitimate parties i.e. CHs and BSs, at proper time. This factor identifies that message can get going to the network or not.

Therefore, the security in sensor networks application is application dependent and different type of applications need different level of security as shown in table 1. However, system must satisfy some basic security requirements. The security and critical application such as intruder detection and border surveillance should satisfy the maximum level of basic security requirements.

Table 1. WSNs security requirements according to different applications

Application	**Confidentiality**	**Integrity**	**Authentication**	**Availability**
Environmental		√	√	
Industrial		√	√	
Healthcare	√	√	√	√
Security/critical	√	√	√	√

3.2. ***Routing Attacks in WSNs***

Due to resources limitations, WSNs exposed to various type of attacks. These attacks can be usually classified into following types: passive and active attacks. In passive attacks, attackers are usually secret and intend to observe the message link to gather the data. The general examples of this type of attacks are eavesdropping, node malfunctioning, node destruction and traffic analysis etc. In active attacks, attackers affect the operations of the network. Network services may put down or terminates as a result. The Denial of Service (DoS), flooding, hole attacks, and Sybil are usual examples of active attacks. The attack could be accomplished from inside, outside, or both, the network. Table 2 list the familiar type of security attacks in WSNs.

These attacks intend to affect the data with one of the following threat [17,18]:

- ***Interruption:*** it is an attack on the network's availability. It's mainly cause system assets unavailable or out of use.
- ***Interception:*** it is an attack on confidentiality. In this type of attack, attacker tries to compromise the network to gain illicit access to the node or data store on it.

- ***Modification:*** it is an attack on system's integrity. In this type of attack the illicit party not only access the data but also change the message content.
- ***Fabrication:*** it is an attack on authentication. The attacker makes an inclusion of messages in the network and consider as it is received from an unauthorized node.

Table 2. Common types of security attacks in WSNs

Name of Attack	**Description**	**Active**	**Passive**	**Inside**	**Outside**
Denial of Service (DoS)	DoS send redundant packets and used extra bandwidth to prevent the legal user from accessing services.	√		√	√
Selective forwarding	It attempts to set a malicious code to be used as usual code and drop the message once they receive this.		√	√	
Sinkhole	It appends a node to network to acquire whole data in case it be a base station.	√		√	
Sybil	The malicious code affirms several identities capable for inter node communication.	√		√	
Wormhole	It put down the messages to a different location and might retransmit it partially or completely.	√		√	√
HELLO flood	It transfers the HELLO packets to the nodes. Main aim of this is more consumption of the network resources.		√	√	
Spoofed, altered or replayed	Here, attacker can obscure the network during some activities like by creating loops or generating fake error messages.	√		√	√
Black-Hole	The malicious node communicate with the target node via false information of rout and put in force it for reply	√		√	
Node Destruction	It either cause node unavailable to replace it with the malicious one, or to prevent it from data collection.	√			√
Eavesdropping	It aims to collect the information about network.		√		√
Traffic Analysis	It aims to intercept and observe messages for e information deduction in patterns for communication.	√			√
Node Replication	It creates duplicate nodes and developed diverse attacks using such nodes.	√			√
Message Corruption	It performs the following main actions: receives message, modifies it, and then forward it.	√		√	√
Jamming	It interfere the node's radio frequencies to make them occupied.	√			√
Node Malfunctioning	It creates erroneous part of data that might depict the integrity of data.	√		√	

4. Secure Clustering in WSNs

Secure clustering process is a sequential process comprised of the following steps: secure cluster head selection (S-CH), secure cluster formation (S-CF), secure data aggregation (S-DA), and secure routing of data (S-DR). Fig.5. depicts a secure clustering process.

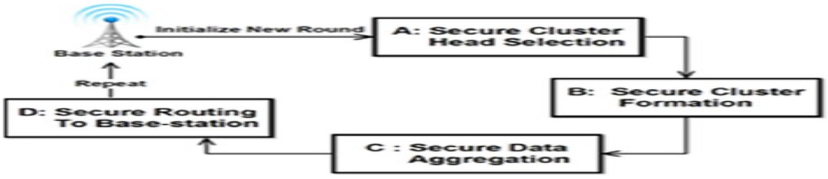
Initialize New Round
A: Secure Cluster Head Selection
Base Station
Repeat
B: Secure Cluster Formation
D: Secure Routing To Base-station
C : Secure Data Aggregation

Figure 5. Secure clustering process in WSNs (Source:[16])

Secure clustering process must guarantees the security goals in each of its phase. Basically, clustering method comprised of following stages: cluster building and data transmission. The former stage begins with the cluster formation in which cluster heads election and nodes allocation are performed. Data transmission intends to protect the data during transfer to BS. So, it consists of following steps: data aggregation and data routing. Data aggregation is the method of transferring the data from nodes to cluster head inside the cluster. Then the CH forward the data to BS through a specific path known a routing process. Finally, the BS receives the data and extracts the meaning, and then the process will be repeated again as shown in fig.5.

To facilitate security for clustering process, there are several security measures such as data partitioning, key management, intruder detection by location or trust management [19,20]. The cryptographic techniques, such as encryption and hashing, are useful in these concerns. However, these schemes greatly increases the energy utilization of the node thus reduce their lifetime [21,22]. So, the key management [23,24,25] is useful especially in the case of asymmetric key schema.

4.1. *Secure clustering protocols in WSNs*

There are lots of routing protocols proposed for wireless sensor networks, most of them are developed without any security consideration, and only few of them deem the problem of security. Most of the papers [26,27,28] specify the general security issue in WSNs like authentication, intrusion detection, secure data aggregation, and secure routing. Only few papers [29,30] deal with the problems of secure clustering and secure CH selection focusing on the issue like dynamic key change, CH election criteria, and complexity. Here in this sub section, we focused on the popular cluster-based routing protocols and their security concerns. On the basis of mechanism used the secure clustering protocols are broadly classified into two categories: cryptography based and data partitioning or multipath based. The popular secure clustering protocols under these schemes are shown in fig.6.

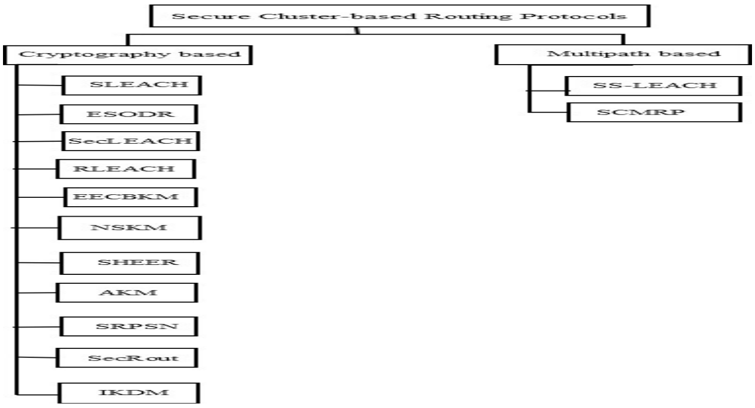

Figure 6. Taxonomy of secure clustering protocols in WSNs

5. Security Analysis

In this section, we performed the analysis of secure cluster-based routing protocols on the basis of various security goals, routing attacks, performance, and cluster build up matrix. Table 3 provides the estimation of these protocols based on robustness and security. Here, we summarize the benefits and restrictions of the above schemes according to perfectness, efficiency, and dynamic clustering criteria. Table 4 represents the above analysis.

Table 3. Secure clustering protocols with security goals

Protocol	**Confidentiality**	**Integrity**	**Authentication**	**Availability**
SLEACH	×	√	√	√
ESODR	√	√	×	√
SecLEACH	√	√	√	√
RLEACH	×	√	√	×
EECBKM	√	√	√	√
NSKM	×	√	√	√
SHEER	√	√	√	√
AKM	√	√	√	√
SRPSN	×	√	√	√
SecRout	×	√	√	√
IKDM	√	√	√	√
SS-LEACH	×	√	×	√
SCMRP	√	√	×	×

Table 4. Secure clustering protocols analysis

Protocol	Mechanism	Perfectness				Efficiency			Nature of Clustering	
		S-CH	S-CF	S-DA	S-DR	M	E	P	D	S
SLEACH	Cryptographic	√	√	×	×	High	Low	Average	√	√
ESODR	Cryptographic	√	√	×	√	High	Low	Low	×	√
SecLEACH	Cryptographic	√	×	√	√	High	Low	Low	√	√
RLEACH	Cryptographic	√	√	√	×	Average	Low	Average	√	√
EECBKM	Cryptographic	√	√	×	×	Low	Low	Low	√	√
NSKM	Cryptographic	√	√	√	×	Low	Average	High	×	√
SHEER	Cryptographic	√	√	×	√	Low	Low	Average	√	√
AKM	Cryptographic	√	√	√	×	Low	Low	High	√	√
SRPSN	Cryptographic	√	√	√	√	Average	Average	Average	√	√
SecRout	Cryptographic	√	√	√	√	Low	Low	High	√	√
IKDM	Cryptographic	√	×	√	√	Low	Low	High	√	√
SS-LEACH	Multi-path	√	√	×	×	High	Average	High	×	√
SCMRP	Multi-path	√	√	√	√	Average	Average	High	×	√

6. Conclusions

Wireless sensor networks have fascinated much concern for both civil and military applications. In these applications a huge number of sensors are needed, requiring careful architecture and network management. To support scalability, grouping nodes into clusters has been popular method in WSNs. In this work, we surveyed the status of research and analyze the different clustering methods. This paper classifies the taxonomy of cluster-based routing protocols. In this work, we focus on security analysis of diverse cluster routing protocols and represent them in tabular form. On the basis of comparison between diverse schemes, it is clear that secure cluster-based routing protocols are much useful in performance improvement of wireless sensor networks. This paper will be very useful for the research group those are interested in the development, modification or optimization of secure routing protocols for WSNs.

Acknowledgments

The author would like to acknowledge ministry of human resource and development (MHRD) for providing financial support for this work under research scholar's grant.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, y., Cyirci, E., “Wireless sensor networks: a survey,” Computer Networks, 2002, Vol. 38, no.4: pp. 393-422.
2. Kazem Sohraby, Daniel Minoli, Taieb Znati, “Wireless Sensor Networks: Technology, Protocols, and Applications,” 2007, John wiley & sons.
3. Yick, J., Biswanath, M., Ghosal, D., “Wireless Sensor Network Survey,” Computer Networks, 2008, Vol.52, Issue 12: pp.2292-2330,.
4. S. Ganesh and R. Amutha, “Efficient and secure routing protocols through SNR based dynamic clustering mechanism,” Journal of Communications and Networks ,2013,15(4): 422-429.
5. S. Soonwha and R. Jaecheol, “ID-based sensor node identification for multilayer sensor network,” Journal of Communications and Networks ,2014,16(4): 363-370.
6. J. Lotf, S. Hossein, N. Ghazan, “Overview of wireless sensor networks,” Journal of Basic and Applied Scientific Research ,2011,11(1): 2811-2816.
7. S. Sahraoui, S. Bouam, “ Secure routing optimization in hierarchical cluster-based wireless sensor networks,” International Journal of Communication Network and Information Security, 2013, Vol. 5, No.3: pp.178-185,.
8. http://monet.postech.ac.kr/images/introduction/image007_new.jpg
9. http://m.eet.com/media/1172006/wisensfig12.3.gif
10. S. Sharma and S. Jena, “ A survey on secure hierarchical routing protocols in wireless sensor networks,” in proceeding of International conference on communication, computing and security, 2011, Rourkela, Odisha, India.
11. Al-Karaki, J.N., and A.E. Kamal, “Routing Techniques in wireless sensor networks: a survey,” IEEE Wireless Communication ,2004,11:6-28,.
12. Kazem Sohraby, Daniel Minoli, Taieb Znati, “Wireless Sensor Networks: Technology: Protocols and Applications,” 2007,John Wiley & Sons.
13. Santar Pal Singh and S.C.Sharma, “A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks,” Elsevier’s Procedia Computer Science , 2015,45: 687-695.
14. Zia, Tanveer and Zomaya, Albert Y., “Algorithms and protocols for wireless sensor networks,” 2009,John Wiley & Sons.
15. Chen Xianqian et al., “ Sensor Network Security: A Survey,” IEEE Communication Surveys & Tutorials ,2009,11: 52-73,.
16. M. Elhoseny, H.K. Elminir, A.M. Riad, X. Yuan, “Recent advances of secure clustering protocols in wireless sensor networks,” , 2014,Vol.2, No.11, pp.400-413.
17. M. Patel and A. Agarwal, “Security attacks in wireless sensor networks: A survey,” in Proceeding of International Conference on Intelligent Systems and Signal Processing, Gujarat,India, 2013,pp.329-333.
18. A. Fuchsberger, “Intrusion detection system and intrusion prevention system,” Elsvier’s Journal Information Security , 2005,10(3): 134-139.
19. M. Zhang, K. Karmani, A. Raghunathan, N. Jha, “Energy efficient and secure data transmission using encompression,” in Proceeding of International Conference on VLSI Design and Embedded Systems, Pune, India, Jan. 2013.

20. A. Semary and M. Abdel-Azim, " A new trends in secure routing protocols in wireless sensor networks," International Journal of Distributed Sensor Networks, 2013.
21. M. Singh and M. Hussain, " A top-down hierarchical multi-hop secure routing protocols for wireless sensor networks," International Journal of Sensor, Ad Hoc and Ubiquitous Computing,2010 1(2): 33-52.
22. E. Sandeep, S. Kusuma, and B. Kumar, "A random key distribution based artificial immune system for security in wireless sesnor networks," in Proceedings of IEEE Students' International Conference on Electrical, Electronics and Computer Science, Japan, 2014.
23. F. Kausar, A. Masood, and S. Hussain, "An authenticated key management scheme for hierarchical wireless sensor networks," Advances in Communication System and Electrical Engineering, 2008, 4: 85-98.
24. Y. Cheng and D. Agarwal, " An improved key distribution mechanism for large scale hierarchical wireless sensor networks," Ad Hoc Networks,2007 5(1): 35-48.
25. P. Zhao, Y. Xu, and M. Nan, "A hybrid Key management scheme based on clustered wireless sensor network," Wireless Sensor Network ,2012,4: 197-201.
26. B. Radhika, P. Raja, C. Joseph, and M. Reji, "Node attribute behavior based intrusion detection in sensor network," International Journal of Engineering and Technology , 2013,5(5): 3692-3698.
27. N. Alrajesh, S. Khan, J. Lloret, and J. Loo, "Secure routing protocol using cross layer design and energy harvesting in wireless sensor networks," International Journal of Distributed Sensor Networks, 2013.
28. G. Wang, D. Kim, and G. Cho, " A secure cluster formation scheme in wireless sensor networks," International Journal of Distributed Sensor Networks, 2012.
29. H. Rifa-Pous and J. Herrara-Joncomart, " A fair and secure cluster formation for ad hoc networks," Wireless Personal Communication, 2011,56(3): 625-636.
30. D. Wu, G. Hu, and G. Ni, " Research and improvement on secure routing protocols in wireless sensor networks," in Proceeding of Fourth IEEE International Conference on Circuit and Systems for Communication, Sanghai, China, 2008, pp.853-856.