

Review of Security Threats in Wireless Sensor Networks

Harjot Kaur¹ Er. Rupinder Kaur² Er. Sangeet Pal Kaur³

¹Research Student ^{2,3}Assistant Professor

^{1,2}Department of Electronics and Communication Engineering

^{1,2}Punjabi University, Patiala, India

Abstract— Wireless sensor nodes are made up of small electronic devices which are capable of sensing, computing and transmitting information from harsh physical environments like a surveillance field. These sensor nodes majorly rely upon batteries for energy, that get depleted at a quicker rate because of the computation and communication operations they have to perform. Wireless Sensor Network (WSN) is a self-configuring type of network in which sensor nodes can join or leave the network when they want. WSN's are usually installed at unprotected and bitter environments where security is an essential issue. In such unprotected environments WSN's are open to many active as well as passive attacks. Security of WSN is very important as such types of networks are generally causing alerts which require sudden attention. False alerts generated by the WSN's may lead to unwanted actions. In this paper various security issues of wireless sensor networks is reviewed and compared in terms of various parameters.

Key words: Intruder Attacks, LEACH, Quality of service (QoS), Security, Sinkhole attack

I. INTRODUCTION

Wireless Sensor Network (WSN) is a combination of tiny light weight wireless sensors with computing elements. These sensor nodes are generally cheaper in price, with limited energy storage and limited processing capabilities. WSN consist of large number of these sensor nodes (usually hundred or thousand of nodes). These types of networks are highly distributed and deployed in hostile environments [1]. WSN's monitor the system or environment by measuring physical parameters such as humidity, pressure and temperature. WSNs are best suited for applications like wildlife monitoring, military command, intelligent communications, industrial quality control, observation of critical infrastructures, smart buildings, distributed robotics, traffic monitoring, examining human heart rates, etc [2].

There are two types of sensors nodes in Wireless Sensor networks, sensor node and a Sink node. A large number of sensor nodes are there in WSN's which collects or sense the data and transmit it to the sink through multiple hops. The sink can use that data locally or globally using internet (as shown in the Fig1.).

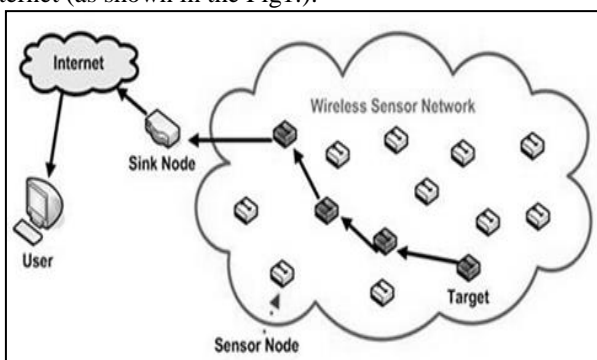


Fig. 1: Wireless Sensor Network

A wide variety of applications of WSN's[3][4] includes in the field of civil and military such as disaster management, video surveillance, intrusion detection, target field imaging and detecting ambient environmental conditions such as temperature, pressure and so on.

In the designing of WSN, we have many challenging issues discussed as below: like communication, power consumption, security, scalability, Quality of Service (QoS) and energy efficiency.

- 1) **Energy Consumption:** Sensor Nodes are dependent on battery power. Sensor networks are placed on hostile environments so replacing the battery is quiet impractical. Hence energy conservation and management is a critical issue to resolve in WSN's [5].
- 2) **Scalability:** The communication protocols in the network must be designed in the way the sensor nodes are deployed whether hundred, thousand or millions of nodes, so that all the deploying nodes in the network do not affect clustering and routing. In other words, the network should preserve its stability [6].
- 3) **Error-prone wireless medium:** Wireless medium can be greatly affected by noisy environments. An attacker causes noise effect to affect the communication and create interference [6].
- 4) **QoS:** One of the major challenges of WSN is to provide consistent Quality of Service (QoS) such as reliability, congestion control, energy efficiency and end-to-end delay, by applying secured routing protocols[7,8,9,10 and 11].
- 5) **Security issues:** Wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping [12].

There are different types of attacks [13] possible in WSN that are classified under two broad categories as follows:

A. Active attacks

Termed as internal and external, it modifies and deletes information. In this dropping, modification, fabrication occurs.

- 1) **Types of Active Attacks:** Grayhole, Information disclosure, Blackhole, sinkhole, Resource consumption.
- 2) **Grayhole:** In Grayhole Attack there is a node in the built up routing topology that selectively drops packet with certain probability causing network distraction. Gray hole may drop packets originating from (or destined to) certain particular node(s) in the network while forwarding every one of the packets for different nodes.
- 3) **Sinkhole Attack:** In this attack the traffic is attracted by the malicious node. The malicious node draws attention of their neighboring nodes by announcing a fake optimal path by using attractive power or bandwidth.

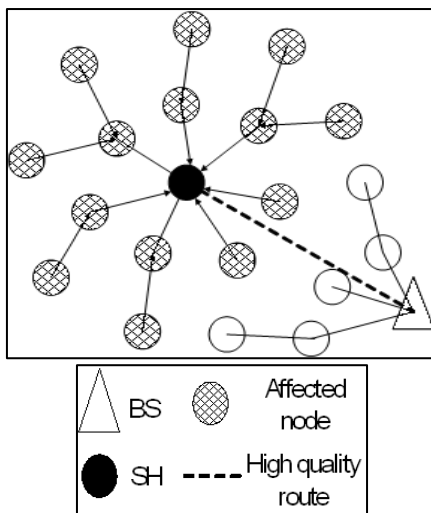


Fig. 5: Sinkhole Attack

III. RELATED WORK

Extensive literature survey has been done related to detection of sinkhole attack & the requirements of QoS in WSN's.

In [1] Yue Liu et.al (2015) proposed "The Mason Test: A Defense against Sinkhole Attacks in Wireless Networks without Trusted Authorities", it describe a technique to use signal prints to detect Sinkhole attack in WSN. The Mason test was implemented on HTC Magic smartphones and tested with human participants in three environments. It eliminates 99.6–100 percent of Sinkhole identities in office environments, 91 percent in a crowded high motion cafeteria, and 96 percent in a high-motion open outdoor atmosphere. [1] "A survey of attacks, Security

Mechanisms and Challenges in Wireless Sensor Networks", the protection goals for sensor networks , various attacks in wireless sensor networks and the security mechanism related to different attacks have been introduced [2]. The paper also presented the challenges of sensor networks.

The message authentication and passing method that is applicable for inspection the trustworthiness or otherwise for a Sinkhole node have been explained by Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal [17]. Duplicate Id and other information of node is only possible when malicious node has all the information of other node. This method is effective and is known for more time consuming than any other method [17]. In order to detect the intruder in a sinkhole attack by an algorithm which firstly finds a group of suspected nodes by analyzing the consistency of data have been introduced in "Detection of Sinkhole Attack in

Wireless Sensor Networks" [18]. The proposed algorithm's performance has been evaluated by using numerical analysis and simulations [18]. An analysis to help network managers understand and assess the various threats associated with the use of wireless technology and a number of available solutions for countering those threats are discussed by Ju young Kim et.al. The different vulnerabilities, threats and attacks that might possibly put WSNs in a vital or critical situation have been identified and discussed in their paper.[14]

The most common security threats in various layers and their most probable solution [15] have been presented by Kalpana Sharma and M K Ghose (2010) in their paper "Wireless Sensor Networks: An Overview on its Security Threats". They have presented the outline of the WSNs threats affecting different layers along with their defense mechanism. They conclude that the defense mechanism presented just gives guidelines about the WSN security threats; the exact solution depends on the type of application the WSN is deployed for[15]. "A Regional Statistics Detection Scheme against Sinkhole Attacks in WSNs",[19], has been proposed by Li, M., Xiong, Y. et.al. The scheme (RSDs) is an effective solution to three key issues: firstly, they address the sinkhole attack by a RSSI-based distributed detection mechanism, secondly, their protocol can prevent the network from a large number of nodes failure caused by sinkhole attacks. Thirdly, the RSDs can maintain a high detection probability with low system overhead by implement experiments [19].

An overview of the security issues, security principles have been proposed by Hero Modares et.al. [20]. The paper represented the different security attacks and demonstrated the different cryptographic techniques [20]. Chun-Hsin Wang and Yang-Tang Li et al. explained in their paper, that malicious nodes may become immediate nodes of routing paths due to replying spoof routing information. Then data packets might be stolen, customized, and even drop by selfish nodes. This type of behavior may affect bandwidth of the resources and consume unnecessary data. So there is a need of modify protocol. In this paper, they proposed a new method to detect malicious nodes actively [21]. "Main Types of Attacks in Wireless Sensor Network", have also been presented by Teodor G. If the security is compromised ,there could be serious penalty starting from theft of information, loss of privacy. So there's a need of a network which is of high privacy and prevent all the attacks in the network [6].

IV. INTRUSION DETECTION ALGORITHM FOR MITIGATING SINKHOLE ATTACK ON LEACH PROTOCOL IN WSN'S

The main objective of this research work is to study the effects of sinkhole attack in a WSN which uses the LEACH protocol for its routing operation and devise a security mechanism to overcome the adverse effects. Sinkholes are triggered in a WSN either by insiders or by an external attacker. The projected IDS algorithmic rule detects the sinkhole attack with high detection rate. The execution of the intrusion detection algorithm is verified numerically and simulations enforce the accuracy and the effectiveness of the algorithm.

A. Low Energy Adaptive Clustering Hierarchy (LEACH) Protocol

A. Pravin Renold et al. [22] states that the routing protocol plays a main role in transmitting the data from source by forming a route to the destination via intermediate nodes and also helps for the effective usage of the power of the nodes when not in the mode of transmission. M. Bala Krishna et al [23] presents that Energy efficient and energy aware protocols in sensor networks are based on the following characteristics:

- 1) Data Aggregation: Data Aggregation collects data samples from a set of sensor nodes
- 2) Data acquisition: Data acquisition collects data samples periodically or event based
- 3) Duty cycle: Duty cycle enables the radio-receiver of a sensor node in sleep or idle state to increase the node life cycle
- 4) Cluster: Cluster is a set of nodes with similar attributes like node distance and signal strength which are grouped together.
- 5) Mobility: It explains that static sensor nodes save more energy as compared to dynamic sensor nodes. Mobile sensor nodes are used if the energy levels of nodes are uneven and enhance the data delivery rate [23].

The main aim of LEACH is to select sensor nodes as CHs by rotation in each round, so the high energy dissipation in communicating with the BS is spread to all sensor nodes in the network.

B. Working Procedure of LEACH

LEACH was proposed by Heinzelman, Chandrakasan and Balakrishnan which is an adaptive clustering algorithm based on hierarchical cluster based routing technique for wireless sensor networks. LEACH organizes the nodes in to clusters. LEACH randomly selects nodes of cluster as cluster-heads (CH) and performs time to time reelection. Cluster Head (CH) responsibility is to create and manipulate a TDMA (Time division multiple access) based schedule and passing aggregated data from each node to the BS where these data is required using CDMA (Code division multiple access). And all the remaining nodes acts as cluster members. The operation of leach protocol is split into two main phases: set up and steady.

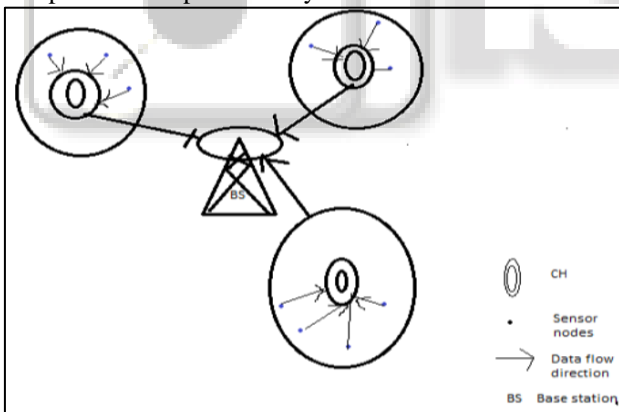


Fig. 6: Architecture of LEACH

C. Two Phases of Leach

LEACH is divided into rounds where each round consists of two phase, set-up phase which is responsible for cluster formation and steady phase which is responsible for data transmission.

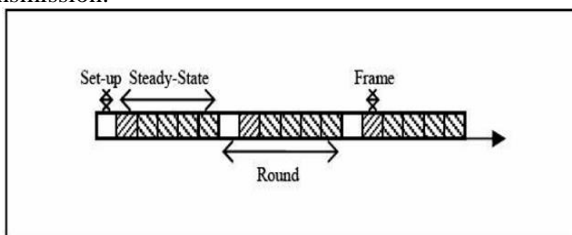


Fig. 7: LEACH protocol phases[24]

- 1) Cluster setup Phase: First step is cluster head selection. At the first of each round, each node selects a random number between 0s and 1 and compares it to the threshold shown in formula. If the selected random number is less than the threshold, the node would be selected as a cluster head for the current round. The threshold $T(n)$ is calculated as:

$$T(n) = \begin{cases} \frac{P}{1 - p(r * \text{mod}(\frac{1}{p}))}, & \text{if } n \in G; \\ 0, & \text{else} \end{cases}$$

Here P is the desired percentage of nodes which are cluster head here, r is the current round, and G is defined as the set of nodes that has not been selected as cluster-heads in the past 1/P rounds. This states that all sensor nodes eventually spend equal energy. After selection of cluster head, it advertises his selection to all remaining nodes. All nodes choose their nearest cluster head when they receive advertisement message based on the received signal strength. Then TDMA schedule is assigned by the CH for their cluster members or nodes. In order to avoid signal interference near the cluster, cluster head can determine the CDMA codes which all nodes used. The CDMA codes which is used in the current phase and TDMA timing information will be sent together. When nodes within the cluster receive the message, they will send data to the cluster head in their own time slot. Algorithm will enter a stable phase.

- 2) Steady Phase: The steady state phase is the data transmission step. During this phase, nodes in each cluster send their data based on the allocated transmission time to their local cluster heads. To reduce the energy dissipation, the receiver of all non-cluster head nodes would be turned off until the nodes' defined allocated time. After receiving all the data from the nodes, the cluster head aggregates all the data sent from the member nodes into a single signal and transfers it to the base station.

V. CONCLUSION

In this paper, various techniques has been reviewed for the reduction of energy consumption in the network. In the network, various types of active and passive attacks are possible. The techniques which are proposed in the previous times has been reviewed and compared in terms of description and outcomes. Future work will focus on improving the performance of the network even after the sinkhole attack occurs by considering the QoS requirements for WSN. To propose a mechanism for prevention and mitigation of sinkhole attack in the network.

REFERENCES

- [1] Yue Liu, David R. Bill, Robert P. Dick, Z. Morley Mao, and Dan S. Wallach, "The Mason Test: A Defense Against Sinkhole Attacks in Wireless Networks Without Trusted Authorities", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 11, NOVEMBER 2015
- [2] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of

- Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, pp. 1-9.
- [3] Deris tiawan, Abdul Hanan Abdullah, Mohd. Yazid dris, "Characterizing Network Intrusion Prevention System", International Journal of Computer Applications (0975 – 8887), Volume 14– No.1, January 2011.
- [4] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks. Ad Hoc Networks", 2015, pp. 325349.
- [5] Chun-Hsin Wang and Yang-Tang Li, "Active Black Holes Detection in Ad-Hoc Wireless Networks", IEEE, 2013
- [6] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.
- [7] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks", Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.
- [8] S. Chen and K. Nahrstedt, "Distributed Quality-of-Service Routing in adhoc Networks", IEEE Journal on Selected areas in Communications, Vol. 17, No. 8, August 2013.
- [9] R. Sivakumar, P. Sinha and V. Bharghavan, "Core extraction distributed ad hoc routing (CEDAR) specification", IETF Internet draft draft-ietf-manetcedar-spec-00.txt, 2014.
- [10] C. R. Lin, "On Demand QoS routing in Multihop Mobile Networks", IEICE Transactions on Communications, July 2010.
- [11] C. Zhu and M. S. Corson, "QoS routing for mobile ad hoc networks", In the Proceedings of IEEE INFOCOM, 2012.
- [12] Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.
- [13] Tumrongwittayapak, C. Varakulsiripunth, R, "Detecting Sinkhole attacks in wireless sensor networks", ICROS-SICE International Joint Conference, pp. 1966–1971 (2009).
- [14] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks", Journal of Security Engineering, 2014, pp.241-250.
- [15] Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010, pp.42-45.
- [16] Venkatraman, K., Vijay Daniel, J., Murugaboopathi, G, "Various attacks in wireless sensor network: survey", Int. J. Soft Comput. Eng. (IJSCE). 3(1), ISSN:2231-2307, 2013.
- [17] G.H. Raghunandan, B.N. Lakshmi, "A Comparative Analysis of Routing Techniques for Wireless Sensor Networks", Proceedings of the National Conference on Innovations in Emerging Technology, IEEE 2011.
- [18] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, "Detection of sink hole Attack in wireless sensor networks", IEEE International Conference on Space Science and Communication (IconSpace), Melaka, Malaysia, 1-3 July 2013, pp. 361-365.
- [19] Li, M., Xiong, Y., Wu, X., Zhou, X., Sun, Y., Chen, S., & Zhu, X., "A Regional Statistics Detection Scheme against Sinkhole Attacks in WSNs", IEEE Sponsored In Trust, Security and Privacy in Computing and Communications (TrustCom), 12th IEEE International Conference on pp. 285-291, 2013.
- [20] Hero Modraes, Rosli Salleh and Amirhossein Moravjosharieh, "Overview of Security Issues in Wireless Sensor Networks", Third International Conference on Computational Intelligence, Modelling and Simulation(CIMSiM), IEEE 2011, pp. 308-311.
- [21] Virendra Pal Singh, Sweta Jain and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.
- [22] A.PravinRenold, R.Poongothai, R.Parthasarathy, "Performance Analysis of LEACH with Gray Hole Attack in Wireless Sensor Networks", IEEE 2012.
- [23] M. Bala Krishnal and M. N. Doja, "Self-Organized Energy Conscious Clustering Protocol for Wireless Sensor Networks", ICACT 2012.
- [24] M. BaniYassein, A. Al-zou'bi, Y. Khamayseh, W. Mardini, "Improvement on LEACH Protocol of Wireless Sensor Network (VLEACH)", International Journal of Digital Content Technology and its Applications, Volume 3, Number 2, June 2009.