Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 11, November 2018, pg.167 – 172

Security Techniques of WSN: A Review

Gaurav Mehta
Research Scholar, Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India
mehtag781@gmail.com

Dr. Parveen Singla
Associate Professor, Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India
parveen.ece@cgc.edu.in

Dr. Rinkesh Mittal
Associate Professor, Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India
hod.coeece@cgc.edu.in

Abstract: ***The wireless sensor node characteristics which include low memory, low computation power, and they are deployed in hostile area and left unattended, small range of communication capability. Based on these characteristics makes this network vulnerable to several attacks, such as sinkhole attack. Sinkhole attack is a type of attack where compromised node tries to attract network traffic. The impacts of sinkhole attack are that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack or altered routing information. It can also use to send fake information to the base station. In this paper we are focus on exploring and analyzing the existing solutions, which are used to detect and identify of the sinkhole attack in wireless sensor network.***
KEYWORDS: WSN, LEACH, Sinkhole

I. Wireless Sensor Networks

Wireless network technology and mobile communications has seen a thriving development as of late. Wireless sensor networks late emerged as a chief research theme. Wireless sensor networks are additionally represents a number of new conceptual and optimization problems,

for example, organization, location and tracking, are fundamental issues, in that numerous applications rely on them for required information [1]. In addition of application demands different classes of networks have merged, for example sensor networks, cellular networks, Ad hoc networks, and mesh networks. They have capacity to transform lives, and system building challenges. Wireless sensors have an excellent tool for military applications, for example intrusion detection, information assembling, perimeter monitoring and support in an obscure deployed area. Different applications are incorporate sensor based location detection with sensor networks, personal health screen and movement detection [2]. Wireless sensor networks having small nodes which send data to base station. Wireless sensor networks are used to track movement of their enemy in military applications. It also used in healthy service for monitoring heart beat and fire detection [3]. Mostly routing protocols do not consider security due to resource constraints which include low power supply, low computational power, low communication range and low memory [4]. Due to this resource constraint creates chances for attackers to easily attack wireless sensor networks. Therefore an example of attack is called sinkhole attack. It is implemented in the network layer, where an adversary tries to attack many traffic. The main aim to prevent base station from receiving a complete sensing data from nodes [5]. In network layer the adversary compromises the node and that node used to launch an attack. The compromised node sending fake information to the neighbor nodes about link quality which used in routing metric help to select best route during data transmission. After data transmission all the packets from his neighbors passed through him before reached to the base station [6]. Sink hole attack prevents the base station from a complete and correct sensing data from nodes.

II. SINKHOLE ATTACK

Sinkhole attack is an insider attack where an intruder compromise a node inside the network and launches an attack. Then the compromise node try to attract all the traffic which coming from neighbor nodes based on the routing metric that used in the routing protocol. Due to the communication pattern in wireless sensor networks in many to one where each node send data to base station, it makes this WSN vulnerable for sinkhole attack [7].

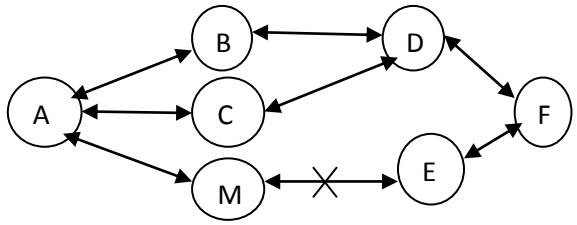

Figure 1: TinyAODV protocol in sinkhole (Teng and Zhang

This technique is used in AODV protocol in launching sinkhole attack.

Sinkhole attack used in Tiny AODV Protocol

In wireless sensor network sinkhole attack is launched under Tiny AODV protocol. This protocol is the same as AODV in MANET but it is lighter as compared to AODV and

modified purposely for wireless sensor network. The routing metric number of hops to base station that used in this protocol. The route from source to destination is created when the node send a request, the source node send a RREQ packet to his neighbor when wants to send packet. The neighbors close to the destination which is reply by sending back RREP (Route Reply) packet, if the packets are not forwarded to other nodes close to that destination. Finally, the source receives RREP packet from the neighbor and select one node with less number of hops to destination. The compromised node or sinkhole node launches an attack by send back RREP packet. In this packet it gives small number of hops which indicates the proximity close to the base station. After the source node decides to forward packet to sinkhole node. The compromised node used the same technique to its neighbors and tries to attract as much traffic as possible [8].

In this figure 1 it shows the node M launches the sinkhole attack in Tiny AODV. After the node A send RREQ to nodes BCM. The node M broadcast to node E like B or C does to node D and it replies back RREP to the node A. After the node A will reject node B and C, then forward the packets to M because node B and A are very far to F compare to the node M.

III. Literature Review

Varshney, k,k [11] "Performance analysis of the malicious nodes in IEEE 802.15.4 based wireless sensor network. " This paper represents to the wireless sensor network. Wireless sensor network is horizontal to many security threats. In wireless sensor network there are large number of attacks like selective forwarding attack, black hole attack, Sybil attack and sinkhole attack. This paper concentrates the performance of this network in the presence of black hole attack by using AD-hoc on demand distance vector routing protocol. In black hole nodes absorbs all messages passing through it. The affected nodes attack the whole traffic and more performance using the AODV without black hole and with black hole attack is analyzed.

Baber Nazir [12] "Mobile sink based routing protocol (MSRP) is used to prolonging lifetime of network in clustered wireless sensor network. " This paper represents the type of sensors near the sink hole to transmit the data for the nodes away from sink hole. They consume their energy very quickly. The wireless sensor network very critical issue for using energy hole or hotspot near the sink. The author mainly focused on the hotspot problem and the purposed mobile sink based routing protocol for network lifetime in clustered wireless sensor network. In MSRP all sink moves in the clustered WSN or collect sensed data from CHs. After gathering the data sink also maintains the sequence about the remaining energy of CHs. Here the author compare with the static sink to the purposed approach or multiple sinks strategies, such as energy per packet. Hence the simulation results demonstrate that MSRP is to be effective for network lifetime as well as improving throughput of multiple sink strategies.

Yulong Zou, et.al proposed in this paper [13], the intercept conduct of industrial wireless sensor network (WSN) is to be comprising of a sink node and multiple sensors within the sight of an eavesdropping attacker. where the sensors are transmit their sensed information to

the sink node using wireless links. Because of the broadcast nature of radio wave propagation, the wireless transmission from the sensors can be overheard by the meddler for interception purposes. An optimal sensor scheduling scheme is to be proposed in this paper to protect wireless transmission against the eavesdropping attack, where a sensor with the highest capacity is scheduled to transmit the sensed information to the sink.

Krontiris et al [14] proposed in this paper to used rule based approach to detect sinkhole attack. They creates the two rules and to be implanted in the Intrusion detection system (IDS). When one of the rules is to violated by one of the nodes, then the intrusion detection system triggered an alarm but it does not provide the node ID of the compromised node. The first rule "For each overhead route which update packet and the ID of sender must be different to your node ID". The second rule "For each and every overhead route update the packet ID of the sender which is one of the node ID in your neighbors".

Coppolino and Spagnuolo [15] proposed in this paper to used hybrid Intrusion detection system to detect the sinkhole attack and other attacks. They are used to detection agent which was responsible for the identifying sinkhole attack. The hybrid intrusion detection system was attached to the sensor node and share resource of that node. The suspicious nodes are inserted to the blacklist which is based on the anomalous behavior after analyzed the collected data from neighbors. Then this list is sent to the central agent who takes the final decision based on feature of attack pattern.

Approach	Proposed Solution	Result	Advantages
Performance analysis based Varshney, k,k 2014 [11]	They concentrate the performance of the network by using distance vector routing protocol.	It absorbs all messages passing through it. Increase the performance of the network.	Affected node attacks the whole traffic and enhance performance of the network.
Mobile sink based routing protocol Baber Nazir 2010 [12]	They proposed in MRSP all sink moves in the clustered WSN or collect sensed data from CHs.	MSRP is to effective for network lifetime as well as improving the throughput of multiple sink strategies.	By using MSRP all sink moves in the clustered WSN. Sink also maintains the sequence about the remaining energy of CHs.
Intercept based Yulong Zou, et.al 2015 [13]	They proposed an optimal sensor scheduling scheme to protect the wireless transmission against the eavesdropping attack.	The broadcast nature of the radio wave propagation a sensor with the highest capacity is scheduled to transmit the sensed information to the sink.	The sensors are to be transmitting their sensed information to the sink node using wireless links. And protect wireless transmission against the eavesdropping attack.

Rule Based. Krontiris et al 2008 [14]	They extended to their Intrusion detection system which can detect the sinkhole attack.	For each and every overhead route update the packet ID of the sender which is one of the node ID in your neighbors	Highly secure and robust measurement based on valuable principle to detect sinkhole attack.
Hybrid Intrusion detection system based Coppolino et al 2010 [15]	They proposed an intrusion detection system which was able to protect the critical information from attacks directs from the wireless sensor network.	In Intrusion detection system they are used to detect agent which is responsible for the identifying sinkhole attack.	The solution satisfied the available resource in sensor nodes and they proved to detect the sinkhole attack.

Table 1: Table of Comparison

IV. Conclusion

Wireless sensor network is a type of network that has been used for sensing information from non-approachable areas. In WSN malicious nodes and are the two main concerned issues. Sinkhole attack is to be performed by attackers degrades performance of the network. Most of the researchers are trying to looking solutions for detecting, identifying and providing resistance to the sinkhole attack in wireless sensor network. Some of the researchers used intrusion detection scheme, other used rule based and key management to detect and identifying the sinkhole nodes. Mostly researches are struggled with the security challenges corresponding with an availability of resources and mobility of wireless sensor nodes. The future solution should focus on reducing computational power, high network overhead, increase detection rate and the system must be validated in real sensor networks.

REFERENCES

[1]. W. Shen, T. Zhang, F. Barac, and M. Gidlund, "PriorityMAC: A priority enhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks," IEEE Trans. Industrial Informatics, vol. 10, no. 1, pp. 824-835, Feb. 2014.

[2]. J.-C. Wang, C.-H. Lin, E. Siahaan, B.-W. Chen, and H.-L. Chuang," Mixed sound event verification on wireless sensor network for home automation," IEEE Trans. Industrial Informatics, vol. 10, no. 1, pp. 803- 812, Feb. 2014.

[3]. Changlong Chen, Min Song, and George Hsieh (2010) Intrusion detection of Sinkhole attack in large scale Wireless Sensor Networks, In Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on (pp.711-716).IEEE

[4]. David Martins and Hervé Guyennet. (2010) Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey, In Network-Based Information Systems (NBiS), 2010 13th International Conference on (pp. 313- 320). IEEE

[5]. P. Samundiswary, D.Sathian and P. Dananjayan. (2010). Secured greedy perimeter stateless routing for wireless sensor networks, International Journal of Ad hoc, Sensor & Ubiquitous Computing(IJASUC)1, (2)

[6]. Pathan, K., AI-S. (2011) Security of SelfOrganizing Networks-MANET, WSN, VANET, WMN. ISB N-13:978-1-4398-1920-3. Taylor and Francis Group.

[7]. Ngai, E., Liu, J and Lyu, M. (2007) An efficient intruder detection algorithm against sinkhole attack in wireless sensor network. Computer Communications, 30(11), 2353-2364
[8]. Teng, L., and Zhang, Y. (2010). Secure Routing Algorithm against Sinkhole attack for Mobile Wireless Sensor Network, In Computer Modeling and Simulation, 2010. ICCMS'10. Second International Conference on (Vol. 4 pp.79-82). IEEE..
[9]. Suman Deb Roy, Sneha Aman Singh, Subhrabrata Choudhury, and N. C. Debnath. (2008). Countering Sinkhole and Black hole Attacks on Sensor Networks using Dynamic Trust Management", In computers and Communications, 2008. ISCC 2008. IEEE Symposium on (pp.537-542). IEEE.
[10]. Jaydip Sen. (2009). A Survey on Wireless Sensor Network Security, International Journal of Communication Networks & Information Security, 1(2).
[11]. Varshney, K.K. "Performance analysis of malicious nodes in IEEE 802.15.4 based wireless sensor network" IEEE International Conference on Information Communication and Embedded Systems, 2014, pp. 1–5.
[12]. Babar Nazir "Mobile Sink based Routing Protocol (MSRP) for Prolonging Network Lifetime in Clustered Wireless Sensor Network" IEEE Conf. on Computer Applications and Industrial Electronics (ICCAIE), 2010, pp. 624–629.
[13]. Yulong Zou, and Gongpu Wang," Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack", 2015, IEEE
[14]. Krontiris,I.,Dimitriou,T.,Giannetsos,T. and Mpasoukos, M. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. In Networking and Communications, 2008. WIMOB'08. IEEE Interational Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.
[15]. Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G.(2010). An intrusion detection system for critical information infrastructures using WSN technologies. In Critical Infrastructure (CRIS), 2010 5th International Conference on (pp. 1-8). IEEE

