A Survey of Various Attacks and Their Security Mechanisms in Wireless Sensor Network

Gursewak Singh, Rajni Bedi

Abstract— ***Wireless Sensor Network (WSN) is an emerging technology with the purpose of demonstrating immense promise for various innovative applications such as traffic surveillance, building, smart homes, habitat monitoring and many more scenarios. The sensing technology joint with dispensation control and wireless communication makes it beneficial for being exploited excess in future. The addition of wireless communication technology as well acquires a variety of security threats. The intention of this paper is to examine the security related problems and challenges in wireless sensor networks. This paper discusses a broad diversity of attacks in wireless sensor network and their classification mechanisms and different security schemes available to handle them as well as the challenges faced.***

Keywords—Wireless Sensor network, Security schemes, Attacks

I. INTRODUCTION

Essentially, sensor networks are application dependent relative. Sensor networks are mainly intended for real-time compilation and analysis of low level information in antagonistic environments [1]. In favor of this motive they are able-bodied suitable to a considerable amount of monitoring and observation applications. Wireless sensor network is self-possessed of hundreds of low-cost sensing devices with computational and communication possessions, and endow with a useful interface among the real world and compassion by means of their data attainment plus dispensation capabilities. Sensor nodes are efficiently arranged and extremely close or within the object to be observed [2], [3]. Wireless sensor network have developed into the idyllic applicant to monitor the physical or environment surroundings in a diversity of applications for instance river pollutants detection, military observation, forest fire monitoring, etc. and their applications are incessantly rising in fame. Except, the major problem that hold back the application of WSN to real-world situations is short of security of its node and communication. Undoubtedly, the information infrastructures, which depend on a WSN with no security pledge, may perhaps even shown the way to disaster [4].

II. WHY SECURITY IN WIRELESS SENSOR NETWORKS

Security in wireless sensor networks is an imperative, significant issue, required and very important requirement, due to:

- WSNs are susceptible against security attacks (Broadcast and wireless environment of transmission medium);
- Nodes installed on hostile environments (insecure physically)
- Unattended nature of WSNs [5]

The main part of this paper is classification of security attacks and security schemes in Wireless Sensor Networks. Section second provides the full information regarding the attacks in Wireless Sensor Networks. Security schemes are discussed in section three. Section four is about conclusion section.

A. Security Attacks

This section describes the very important discussions on most dangerous attacks

1) Eavesdropping Attack:

The eavesdropping attack is very serious security threat in the direction of a wireless sensor network because the eavesdropping attack is a precondition for other attacks. Conservative WSNs consist of wireless nodes with unidirectional antennas, which transmit radio signals in all directions and are subsequently prone to the eavesdropping attacks [6]. Different from unidirectional antennas, directional antennas give out radio signals on needed directions and potentially decrease the opportunity of the eavesdropping attacks. The eavesdropping attacks have two types active and passive. Passive attack is the unauthorized, covert monitoring of transmissions. Man in middle attack is an active type of eavesdropping attack. In this attack the attacker create independent connections through the victims and communicate messages between them, making them consider so as to they are talking openly to each other in excess of a confidential connection.

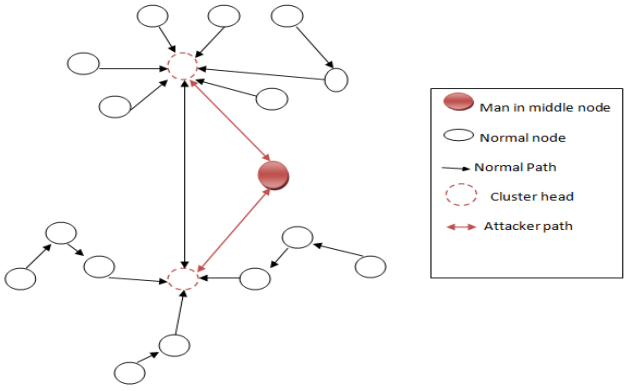

Fig. 1 Man in Middle Attack

2) Sinkhole Attack:

In this adversary plan is to attract almost all the traffic from a specific region through a compromised node, generating a symbolic sinkhole by the opponent at the centre. Sinkhole attacks normally work by making a compromise node appear particularly striking to

Manuscript Received on June 19, 2014.

Gursewak Singh, Received the B.Tech Degree in Computer Science Engineering from Punjab Technical University, India.

Rajni Bedi, Received the B.Tech degree in computer science and engineering from Guru Nanak Dev University, India.

adjacent nodes with respect to the routing algorithm. Sinkhole attacks are hard to counter since routing information supplied by a node is difficult to prove. As an example, a laptop-class adversary has a strong power radio transmitter to permit it to give an expert route by transmitting with sufficient power to arrive at a wide area of the network.

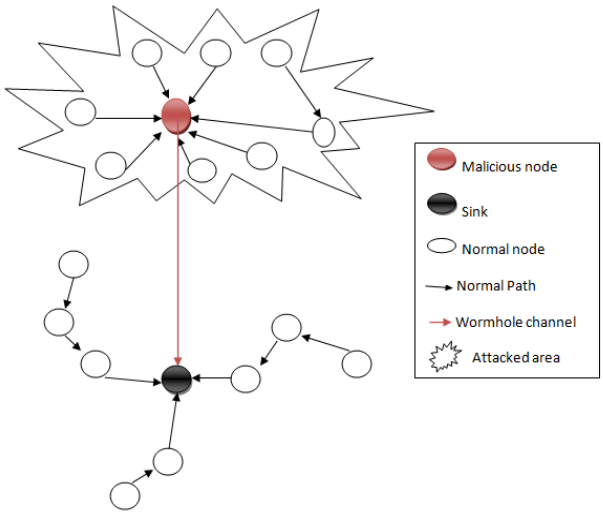

Fig. 2 Sinkhole Attack

3) Sybil Attack:

The Sybil attack is defined as a malicious device illegally captivating on multiple identities. A solitary node duplicates itself and obtainable in the manifold locations. The Sybil attack is intention fault tolerant method for instance distributed storage, multipath routing and topology preservation. Sybil attack, a solitary node represents multiple identities to additional nodes in the network [7], [8]. Verification and encryption techniques are able to prevent an unknown to initiate a Sybil attack.

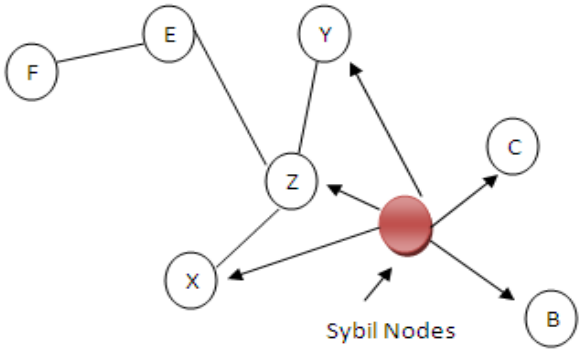

Fig. 3 Sybil Attack

4) HELLO Flood Attack:

An attacker sends or repeats a routing protocol's HELLO packets beginning one node to another via extra energy. This attack makes use of HELLO packets as a weapon to induce the sensors in wireless sensor network. In this kind of attack an attacker with a very high radio transmission range and dispensation control send HELLO packets to a number of sensor nodes with the intention of inaccessible in a large area within a WSN. The sensors are therefore prejudiced that the adversary is their neighbor [9]. As a result, at the same time as sending the information to the base station, the victim nodes attempt to go from side to side the attacker as they be acquainted with that it is their neighbor and are eventually spoofed by the attacker.

5) Node Replication Attacks:

In node replication attack an attacker seeks to insert a node to a presented sensor network by replication the node ID of an available sensor node. A node pretended in this approach is able to strictly disrupt a sensor network's performance. Packets can be misrouted or damaged. Due to this it results in disconnected network and false sensor readings. If an attacker is able to increase physical access to the whole network the attacker copy cryptographic keys to the pretended sensor nodes [10]. By adding the replicated nodes at exact network points, the attacker might easily influence a specific section of the network, maybe by disconnecting it overall.

III. SECURITY SCHEMES

A. Secure Key Management Scheme for Eavesdropping Attack

For eavesdropping attack in WSN the main security scheme is secure key management. Under this scheme many protocols are present in computer world which provide the security to sensor nodes for example diffie-hellman key exchange protocol. In this scheme the every node sends the information to another node. That information is in the encrypted form and can be decrypted by using the keys. These keys are either symmetric or asymmetric according to the network scenario [13]. This scheme protects the data of sensor nodes. The malicious nodes can't understand the data because the data is in encrypted form and can be decrypted only by using the secured keys.

B. REWARD Security Scheme for Sinkhole Attack

The idea of Reward (receives, watch and redirect) is associated with the replication technology. In this scheme every node's transmission is directed to instantaneous neighbors, solitary node forward and one node toward the back. If a node try a Sinkhole attack and drop a package, it will be detected through the next node within the path. All nodes in wireless sensor network tune the broadcast power to arrive at both instant neighbors. The nodes broadcast packets as well as observe if the packets are forwarded. If malicious nodes do not perform as a forwarder, the preceding node within the path will transmit a SAMBA message. The viewer wait for a predefined time period, transmits the packet changing the path as well as broadcasts a SAMBA (distrustful area, mark a sinkhole attack) message [16]. The SAMBA message gives the location of the sinkhole attack. In order of maximum value of the flooding to the nodes situated in a close surrounding area of the malicious node, SAMBA have a counter which is decremented on every node prior to retransmission. While the counter finishes, the retransmission is ended. Therefore, a group of nodes in the region of the malicious node will also avoid the area or else use REWARD to go through.

C. Radio Resource Testing, Random Key Pre-distribution Security Schemes for Sybil Attack

If we want to provide the protection to sensor nodes against the sybil attack then we have to validate the sensor nodes. There are main two methods to validate an identity [11]. The first form is the direct validation, in which a node openly tests whether another node identity is valid or suitable. The second type is indirect validation, in which nodes that have already been confirmed are allowed to guarantee for or else refute other nodes. The radio resource testing is used in direct validation method. In this the radio resource testing is considered for the purpose of a node needs to verify that none of its neighbors are Sybil identities. It can allocate each of its 'n' neighbors a different channel to broadcast a number of messages on. It can then choose a channel randomly scheduled on which to listen. If the neighbor that was assigned that channel is genuine, it should hear the message otherwise not. And in the random key pre-distribution, in the key set-up stage, every node is able to discover or calculate the general keys that are allocated by its neighbors. The common keys will be used as a shared secret session key to make sure node-to-node secrecy.

D. Bidirectional Verification Security Scheme for HELLO Flood Attack

A lot of protocols need nodes to transmit HELLO packets to broadcast themselves in the route of their neighbors, as well as a node in receipt of such a packet can assume that it is surrounded by normal radio range of the sender. This supposition may be fake; a laptop-class attacker broadcasting routing or else extra information by large sufficient transmission power might induce each node in the network that the opponent is its neighbor. To begin this type of attack, an adversary packet distribution range should be bigger than a normal node sending range. But every sensor node creates a set of available neighbor nodes, as well as merely ready to receive request messages from this set of neighbor nodes, then request messages as of an opponent transmitted with larger power will be unobserved [12]. Thus, the harm from a HELLO flood attack can be controlled within a minute range. To protect aligned with this attack, every request message forward through a node is encrypted with a key. The new encryption key is generated during communication. In this method, several nodes accessible neighbors are able to decrypt and confirm the request message while the attacker will not be acquainted with the key and will be prevented from initiation the attack.

E. Localized Approach, Centralized Approach, and Distributed Approach Security Scheme for Node Replication Attacks

This approach cannot sense the dispersed node duplication where the replicated nodes are extra than two hops away. Other technique that is able to dependably notice the node replication is based on central approach. At this point every node sends its neighbor's claimed location information to the base station for verification [14]. This method can effectively detect the node replication attack but nodes close to the base station stand the force of extreme communication. As well nodes close to the base station are focus to rebellion by the attacker as failure of these nodes cripples the WSN [15]. Therefore distributed approach where each and every node in the WSN share the load of detection, is the majority preferred solution. Different protocols are used to detect the replicated node under distributed approach like randomized multicast protocol.

IV. CONCLUSION

Generally most of the attacks beside security in wireless sensor networks are caused by insertion of fake data or information through the compromise nodes inside the network. For shielding the inclusion of fake information by compromise nodes, a means is necessary for sensing fake information. On the other hand, developing such a detection mechanism and creating it proficient signifies an immense research challenge. This paper described the attacks and their classifications in wireless sensor networks as well as makes an effort to discover the security mechanism extensively use to handle these attacks. So this survey will optimistically inspire future researchers to arise with smarter as well as more robust security methods and create their network safer.

REFERENCES

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.
2. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks" Communications Magazine,IEEE, vol. 40, pp. 102-114, 2002.
3. Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey," *Computer Networks,Elsevier*, vol. 52, pp. 2292-2330, 2008.
4. D. Culler, D. Estrin, M.Srivastava, "Overview of Sensor Networks," *Computer Magazine,IEEE*, vol. 37, no. 8, pp. 41-49, August 2004.
5. S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks,DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009
6. Al-Sakib Khan Pathan, Hyung-Woo Lee "Security in Wireless Sensor Networks: Issues and Challenges" ISBN 89-5519-129-4, ICACT2006
7. J.N.Al-Karaki, Raza Ul-Mustafa, Ahmed E. Kamal, "Data Aggregation in Wireless Sensor Networks -Exact and Approximate Algorithms," in *Proceedings of IEEE Workshop on High Performance Switching and Routing (HPSR)*, Phoenix, Arizona, USA, 2004, pp. 241-245.
8. A.W. Krings Z. (Sam) Ma, "Bio-Inspired Computing and Communication in Wireless Ad Hoc and Sensor Networks," Ad Hoc Networks,Elsevier, vol. 7, no. 4, pp. 742-755 , June 2009.
9. Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal,Special Issue on Sensor Network Applications and Protocols, September2003, pp. 293-315.
10. Karlof, C., Sastry, N., and Wagner, D., "TinySec: a link layer security architecture for wireless sensor networks", Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD,USA, 2004, pp. 162 – 175.
11. Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004,pp. 259 – 268.
12. Hamid, M. A., Rashid, M-O., and Hong, C. S., "Routing Security in Sensor Network: Hello Flood Attack and Defense", to appear in IEEEICNEWS 2006, 2-4 January, Dhaka.
13. Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless SensorNetworks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.
14. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., and Srivastava, M.B., "On communication security in wireless ad-hoc sensor networks", 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002, 10-12 June 2002, pp.139 – 144

15. Kulkarni, S. S., Gouda, M. G., and Arora, A., “Secret instantiation in adhoc networks,” Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, May 2005, pp. 1–15.
16. Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.

AUTHORS PROFILE

Gursewak Singh Received the B.Tech degree in computer science engineering from Punjab technical university, India, in 2011. He has done his M.Tech degree in computer science and engineering from lovely professional university, India, in 2013. His research interest includes RFID (radio frequency identification), Security analysis of RFID system and Cryptography algorithms for RFID, key redistribution schemes and Security schemes in wireless sensor networks and network security protocols design.

Rajni Bedi Received the B.Tech degree in computer science and engineering from Guru Nanak Dev University, India, in 1998. She has done his M.Tech degree in computer science and engineering from Punjab Agriculture University, India, in 2001. Her research interest includes Analysis of Algorithms, Data Mining and object Oriented Analysis and Design, Computer Networks.