Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Challenges and Security Attacks in Wireless Sensor Network

Harmeeet Singh
Deptt. of Computer Application
Jalandhar, Punjab, India

Abstract—Recent advances in technology has made researchers quite optimistic towards the feasibility of Wireless sensor networks (WSNs). WSN is an emerging technology that shows great promise for various futuristic applications both for mass military and public. In this article we present a survey of challenges and attacks in WSNs. First we outline the challenges and then attacks with their corresponding countermeasures in WSNs. In this paper, our center of attention is on attacks and issues in WSNs.

Keywords— Wireless Sensor network (WSNs ; security ; attack; challenges.

I. INTRODUCTION

Recent advances in wireless communication and electronics have enabled the development of multifunctional sensor nodes, low power, low-cost. These tiny sensor nodes, consisting of data processing, communication and sensing components, make it possible to deploy WSNs, which represent a significant improvement over traditional WSNs. WSNs can simplify operation and system design, as the environment being monitored does not require the energy or communication infrastructure associated with wired networks [1].

Wireless sensors are equipped with a set of transducers and a radio transceiver through which they acquire information about the surrounding environment. During deployed in large quantities, these sensors can automatically organize themselves to form an ad hoc multihop network to communicate with each other and with one or more sink nodes. Remote user can inject commands into the sensor network via the sink to assign processing, transfer and data collection tasks to the sensors, and it can later receive the data sensed by the network through the sink.

A diverse set of applications for sensor networks encompassing different fields have already emerged including military, inventory monitoring, agriculture, medicine, environment, motion tracking, intrusion detection, toys and many others. Use of this technology appears to be limited only by our imagination and ingenuity.

In pollution detection systems WSNs can also monitor the current levels of polluting substances in a town or a river and identify the source of anomalous situations, if any. Similar detection systems can be employed to monitor water levels and rain and fire, prevent flooding or other natural disasters [2].

In the medical field WSNs can be used to remotely and unobtrusively monitor physiological parameters of patients such as heartbeat or blood pressure, and report to the hospital when some parameters are altered.

Another possible application that was recently experimented is the monitoring of animal species and collection of data concerning their population, habits or position. Sensors can be deployed to continuously report environmental data for long periods of time. It is a very important improvement with respect to previous operating conditions where humans had to operate in the fields and periodically take manual measurements resulting in fewer data, higher costs, higher errors and non negligible interference with life conditions of the observed species.

While some aspects of WSNs are similar to traditional wireless ad hoc networks, important difference exist which greatly affect how security is obtained. The differences between sensor networks and ad hoc networks are:

- Sensor nodes are densely deployed.
- The topology of a WSNs changes very frequently due to mobility or failures.
- Sensor nodes are limited in memory, computation and power resources.
- The number of nodes in a WSN can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are engaged to failures due to harsh environments and energy constraints.

II. CHALLENGES IN WLAN

WSNs security challenges – When a wireless network is established, design a secure network is a concern. WSN security challenges are:

A. Easy Access

The nature of a wireless network is to provide easy access to end users, Strictly speaking this is not a security threat but this ease of access creates a more open attack surface. The wired network that requires an attacker to physically access part of the network, information available about WSNs is also the information needed to launch an attack on the network, a WSNs only requires that the attacker be in close proximity.

B. Rogue Access Points (AP)/Ad-hoc networks

A Rogue AP is an access point that has been installed on a secure network without explicit authorization from a system's administrator. Rogue access points pretense a security threat because anyone with access to the premises can ignorantly or maliciously install an inexpensive wireless AP
that can potentially allow unauthorized parties to access the network.

C. Unauthorized Use of Services

Most of the AP's running with default configurations have not activated with Wired Equivalent Privacy (WEP) [3].

D. Configuration Problems

Simple configuration problems are often the cause of many vulnerabilities, this is because many consumer, Small Office, Home Office grade access points with no security configuration. A new user can set up one of these devices quickly and gain access. They also open up their network to external use without further configuration .Other potential issues with configuration include weak passphrases, weak security deployments (i.e. WEP vs WPA vs WPA2), and default SSID usage among others.

E. Services and Performance Constraints

WLAN have limited transmission capacity. If an attacker were to launch a ping flood from a fast Ethernet segment it could easily overwhelm the capacity of an AP.

F. MAC Spoofing

MAC spoofing occurs when an attacker alters the MAC address of their host to match another known MAC address of a target host. 802.11 networks do not authenticate frames. There is no protection against forgery of frame sources that addresses, the attacking host then sends a frame throughout the network with the newly configured MAC address. Attackers can use spoofed frames to redirect traffic and corrupt address resolution protocol (ARP) tables. An attacker on a fast enough host can capture and forward packets so that victims do not notice any change in their network access. It then inadvertently forwards frames destined for the target host to the attacking host.

G. Session Hijacking

Session hijacking is a method of taking over a Web user session by surreptitiously obtaining the session ID masquerading as the authorized user. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and do anything the user is authorized to do on the network.

H. Traffic Analysis and Eaves Dropping

802.11 provide no protection against attacks that passively observe traffic [4]. The main risk is that 802.11 do not provide a way to secure data in transit against eavesdropping [5].

I. Higher Level Attacks

Once an attacker gains access to a wireless network it can serve as a launch point for attacks on other systems.

III. ATTACKS IN WSNS

WSNs are susceptible to security attacks due to the broadcast nature of the transmission medium. WSNs have an additional vulnerability because nodes are often placed in a dangerous environment or adversary where they are not physically protected. Here we point out the major attacks in WSNs

A. Denial of Service

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action [6], [7] . A DoS is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic .The simplest DoS attack tries to exhaust the resources available to the node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. .Denial of Service attacks is termed one of the worst attacks and is next to impossible to track .DoS attack is meant not only for the adversary's attempt to destroy ,disrupt or subvert a network, but also for any event that diminishes a network's capability to provide a service. Several types of DoS attacks in different layers in WSNs, might be performed. At physical layer the DoS attacks could be tampering and jamming, at link layer, exhaustion, unfairness, collision, at network layer, misdirection ,greed and neglect, homing, black holes and at transport layer this attack could be performed by desynchronization and malicious flooding. The mechanisms to prevent DoS attacks include payment for network resources, strong authentication, pushback and identification of traffic.

B. Attacks on Information in Transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirements .During sending the report, the information in transit may be spoofed, replayed again or vanished and altered. In wireless communication any attacker can monitor the traffic flow and get into action to intercept, modify ,interrupt or fabricate packets [8] , provide wrong information to the base stations or sinks, vulnerable to eavesdropping.

Sensor nodes typically have scarce resource and short range of transmission , an attacker with high processing power and larger communication range could attack several sensors at the same time to modify the actual information during transmission.

C. Sybil Attack

In many cases, the sensors in a WSNs might need to work together to fulfill a task, hence they can use redundancy of information and distribution of subtasks. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes (Figure 1). This type of attack where a node forges the identities of more than one node is the Sybil attack [9]. Sybil attack tries to degrade the security , resource utilization and integrity of data . Sybil attack can be performed for attacking the data aggregation, routing mechanism, voting, distributed storage, misbehavior detection [10] and fair resource allocation. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to sybil attack. WSNs can have some sort of gateways or base stations, this attack could be prevented using accomplished protocols. Douceur showed that, Sybil attacks are always possible except under extreme and unrealistic assumptions of coordination and resource parity among entities, without a logically centralized authority [9]. Newsome et. al. [10] used radio resource testing to detect the presence of sybil node(s) in sensor network and showed that the probability to detect the existence of a sybil node is:

$$\Pr(detection) = 1 - \left(1 - \sum_{all\ S,M,G} \frac{\binom{s}{M}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}}^{S-(m-M)}_{c}\right)^{r}$$

here, *s* is the number of sybil nodes, *g* number of good nodes, *M* are malicious (faulty) nodes, *m* malicious nodes, *n* is the number of nodes in a neighbor set, *c* is the number of nodes that can be tested at a time by a node, of which *S* are sybil nodes, *G* are good (correct) nodes and *r* is the number of rounds to iterate the test.

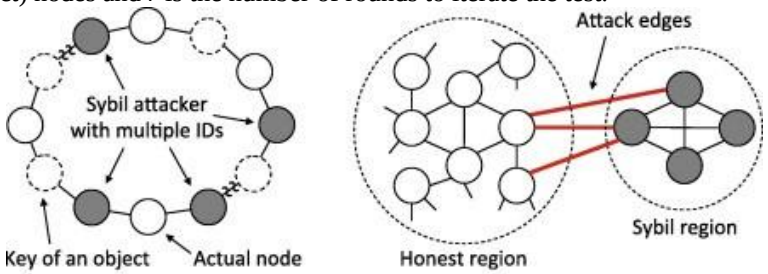

Fig. 1. Sybil Attack [5]

D. Blackhole/Sinkhole Attack

The black hole attack is one of the well-known security attack in WSNs . In this attack, a malicious node acts as a blackhole to attract all the traffic in the sensor network [11] . Specifically in a flooding based protocol, the intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. . A single black hole attack is easily happened in the WSNs [11]. An example is shown as Figure 2, node 1 represents the source node and node 4 stands for the destination node. Node 3 is a defect node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 mistakenly judges the route discovery process with completion, and starts to send data packets to node 3. Once the inimical device has been able to insert itself between the communicating nodes (for example, sensor and sink node), it is able to do anything with the packets passing between them. This attack can affect even the nodes those are considerably far from the base stations.

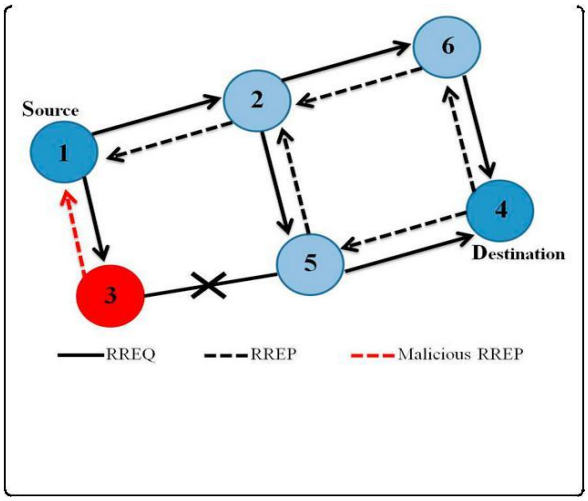

Fig. 2. The single black hole problem. [11]

Figure 2 is an example of single black hole attack in the mobile ad hoc networks [11]. Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node1 erroneously judges the route discovery process with completion and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in WSN's. As a result, node 3 is able to misroute the packets easily and the network operation is suffered from this problem.

E. Wormhole Attack

Wormhole attack is a critical attack in which the attacker records the packets (or bits) at part of the network over a low latency link and replays them in a different part of the network [12]. The retransmitting or tunneling of bits could be done selectively. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. The tunnel can be established in many different ways, such as through packet encapsulation, high powered transmission or out-of band hidden channel (e.g., a wired link). Wormhole attack is a threat to WSNs, because; this sort of attack could be performed even at the initial phase when the sensors start to discover the neighboring information. The wormhole attack mainly consists in network layer attacks.

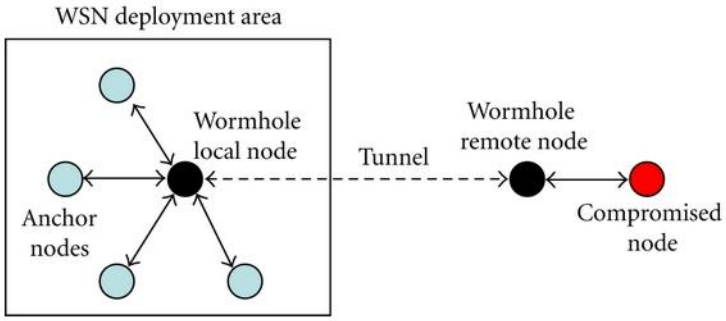

Fig. 3. Wormhole Attack [12]

Worm hole node fake a route that is shorter than the original one within the network ; this can confuse routing mechanisms which rely on the knowledge about distance between nodes. It has one or more malicious nodes and a tunnel between them . The attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally . A wormhole attack can easily be launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms.

F. Hello Flood Attack

Hello Flood Attack is introduced in [13]. Some routing protocols in WSN require nodes to broadcast hello packets to announce themselves to their neighbors. This attack uses HELLO packets as a weapon to convince the sensors in WSN. A node which receives such a packets may assume that it is within a radio range of the sender. In this sort of attack an attacker with a high radio transmission range (termed as a laptop-class attacker broadcasting routing) and processing power sends HELLO packets to a number of sensor nodes which are diffused in a large area within a WSN. The sensors are thus reassure that the opposing is their neighbor. As a result, While sending the information to the base station, as the victim node know that the adversary is their neighbor and try to go through the attacker and are ultimately spoofed by the attacker.

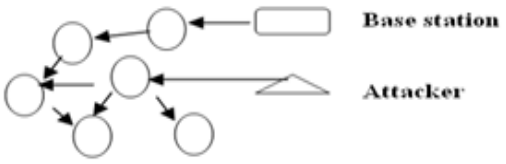

Fig. 4(a) [13]

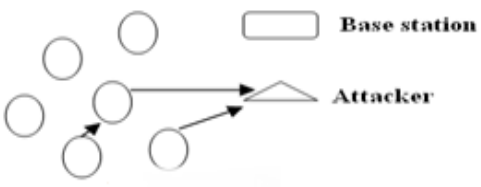

Fig. 4(b) [13]

Figure 4(a) shows an attacker broadcasting hello packets with more transmission power than a base station. Figure 4(b) shows that a legitimate node considers attacker as its neighbour and also as an initiator.

IV. CONCLUSION

WSNs have created wide range of challenges that still needs to be addressed. In this paper we have identified a comprehensive list of challenges associated with WSNs . We have also discussed some popular attacks in WSNs. Most of the attacks against security in WSNs are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. The impact of WSNs on our day to day life can be preferably compared to what Internet has done to us. This field is surely going to give us tremendous opportunity to change the way we perceive the world today.

REFERENCES

[1] D. Estrin *et al.*, "Instrumenting the World with Wireless Sensor Networks," *Proc. Int'l. Conf. Acoustics, Speech and Signal Processing*, Salt Lake City, UT, May 2001.

[2] David C. Steere, Antonio Baptista, Dylan McNamee, Calton Pu, Jonathan Walpole, "Research Challenges in Environmental Observation and Forecasting Systems", Proc. 6th International Conference on Mobile Computing and Networking (MobiCom 2000), pp. 292-299, Boston, MA, USA August 2000.

[3] David; Security of the WEP algorithm; March 4, 2005; http://www.isaac.cs.berkeley.edu/isaac/wepfaq.Html

[4] RIVEST,R.,RSA Security response to weaknesses in keyschedulingalgorithm of RC4, http://www.rsasecurity.com/rsalabs/technotes/wep.html, 2001.

[5] BORISOV, N., GOLDBERG, I., AND WAGNER, D.,Intercepting mobile communications: The insecurity of 802.11, 2001.

[6] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003,

pp. 26 – 36.

[7] Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[8] Pfleeger, C. P. and Pfleeger, S. L., "Security in Computing", 3rd edition, Prentice Hall 2003.

[9] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[10] 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.

[11] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[12] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[13] 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, September 2003, pp. 293-315.

AUTHOR PROFILE

Mr. Harmeeet Singh is presently pursuing Ph.d in field of Wireless Sensor Networks from PTU . The degree of MCA from DAVIET Jalandhar .Research Interest includes Data Structure , Network Security and Cloud Computing. Object Oriented Technology and Computer Graphics & Multimedia.
Mobile: +91-7508000449
E-mail: harmeetsingh143@yahoo.co.in

