ISSN :2455-0108 IJO–Science Impact Factor : 2015-3.462
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II, Issue VIII November 2016

SECURITY ISSUES IN WIRELESS SENSOR NETWORKS – AN OVERVIEW

PANKAJ
NET (COMPUTER SCIENCE & APPLICATIONS)
B.TECH. (IT)
MCA
MBA (IT & MARKETING)
MAHARSHI DAYANAND UNIVERSITY, ROHTAK
HARYANA
INDIA

Abstract

A wireless sensor network (WSN) is a spatially distributed autonomous sensor to monitor and cooperatively report information about physical or environmental conditions, such as temperature, sound, pressure, etc. through the network to a server machine. WSNs are typically enforced for assembling data from insecure surroundings. Nearly all security protocols for WSN believe that the unwelcome person is able to do entirely management over a detector node by manner of direct physical access. The looks of detector networks together of the most technology within the future has display numerous challenges to researchers. The challenges thrown by WSNs are distinctive given their delicate design and scant resources. Even supposing security for wireless networks has been a wide researched space for several decades, security for WSNs continues to be a serious roadblock for his or her potency and performance.

Keywords—Wireless detector networks; security; WSN; barrier coverage; intrusion detection system; IDS.

I. **Introduction:**

The safety problems in wireless detector network is thanks to the struggle of what proportion resources is spent for security in proportion to the detector application. this security perspective for WSNs is on a per-attack basis, that creates AN inflexible model leading to poor potency and measurability. making a security framework giving high flexibility, sensible measurability and a redundancy-free security layer for the WSN protocol stack and relies on a resource perspective once deciding security solutions, wherever solutions ar designed to secure every resource within the WSN surroundings, instead of defend against attacks.

A. Intrusion detection system

There ar several challenges to the safety in wireless detector network and it's thanks to some reasons just like the nature of knowledge transfer of wireless communication, restricted resources of detector nodes, unattended things wherever detector nodes may well be at risk of physical attack, etc. to reinforce the safety of wireless detector networks authentication techniques, cryptography techniques is used. These solutions alone will ne'er stop all attainable attacks. therefore a second level of security is Intrusion Detection Systems (IDS) [4]. B. Secure localization in wireless detector networks unexpected wireless detector networks (WSNs) have attracted a good deal of attention in recent years for his or her broad potential in each military and civilian operations. the right operations of the many WSNs think about the information of physical detector locations. However, most existing localization algorithms developed for WSNs ar at risk of attacks in hostile environments. As a result, adversaries will simply subvert the conventional functionalities of locationdependent WSNs by exploiting the weakness of localization algorithms. during this paper, we tend to 1st gift a general secure localization theme to shield localization from adversarial attacks. we tend to then propose a mobility assisted secure localization framework for WSN.

B. Intrusion detection and privacy

Wireless detector networks typically got to be protected not solely against an energetic assaulter United Nations agency tries to disrupt a network operation, however additionally against a passive assaulter United Nations agency tries to urge sensitive data regarding the situation of an exact node or regarding the movement of a half-tracked object. to deal with these problems, we are able to use AN intrusion detection system and a privacy mechanism at the same time. However, each of those typically accompany contradictory aims. A privacy mechanism generally tries to cover a relation between numerous events whereas AN intrusion detection system (IDS) tries to link the events up. Here, we tend to 1st explore many issues which will seem once each AN intrusion detection system and a privacy mechanism ar used within the network. There ar issues which may occur once each IDSs and privacy mechanisms ar used at the same time.

Problem causes to IDS-

Privacy mechanisms typically purposely hide the identity of nodes, assign multiple pseudonyms to one node or use dynamically dynamical pseudonyms. therefore one node might have totally different|completely different} pseudonyms for communication with different neighbors and these pseudonyms might modification in time. Packets sent by the node then contain identifiers that ar perceivable solely to the present node and therefore the supposed recipient. this could cause hassle to AN ID since it's not capable to link overheard packets with a specific sender or recipient. The IDS will not be ready to decide whether or not the proclaimed pseudonym of a node is true ?

Privacy mechanisms make a mess in a network by hiding identities of nodes, introducing new traffic, etc. Privacy mechanisms would possibly share some (secret) data with AN IDS, above all ought to this sharing facilitate the IDS to arrange the mess" and with success find active attackers. a haul to unravel is that an exact IDS node might accumulate plenty of secret data, changing into a sweet spot for AN assaulter. the subsequent approaches to sharing is taken.

Pre-shared secret-

Privacy mechanisms use a trapdoor perform for nom de guerre generation, content protection or dummy traffic identification. The trapdoor data is pre-shared between a privacy mechanism ANd an IDS, therefore the IDS is aware of all the data necessary to run properly. No any cooperation is required. However, the IDS knowing the trapdoor data is tempting for AN assaulter. The impact of AN IDS compromise is reduced by sharing solely partial data or data that's valid just for an exact time.

2. Delayed information disclosure:

Certain information is retrospectively revealed by privacy mechanisms, especially if this information helps the IDS to understand audit data recorded in the past. This approach assumes that an attacker needs the information immediately and delayed disclosure is not helpful for her. This approach can be used, for example, to retrospectively differentiate dummy and real traffic.

3. Information is revealed on demand:

The information necessary to cancel the effect of privacy mechanisms' protective actions can be obtained by an IDS on demand, if the IDS executes an additional protocol and a privacy mechanism cooperates. The key characteristics are that IDSs cannot obtain the information without cooperation of privacy mechanisms and the obtained information is limited to cancelling effects of privacy mechanism protective actions only for a certain subject or time period (one message, one identity, etc.).

4. Threshold scheme for information availability:

Information available to an IDS running on a particular node is intentionally limited to provide additional resilience against the node compromise. To obtain full information required, multiple nodes with an IDS/privacy mechanism must cooperate, potentially with the support of a suitable cryptographic threshold scheme.

IDS Leverage Co-existence of IDSs and privacy mechanisms may benefit both when used properly. If an IDS has several identities, it can, for example, send a probing message (using one identity) that should be forwarded back to itself (represented by another identity). These probing messages increase the amount of traffic and may play the role of dummy traffic. This also makes the traffic analysis harder and helps the privacy mechanism. Another benefit is that an attacker cannot easily avoid an IDS by selecting one (static) path without IDSs if a privacy mechanism ensures that multiple routes or randomly chosen routes are used.

II. Attacks On Sensor Networks

Wireless sensor networks are not limited to simply denial of service attacks, but rather encompass a variety of techniques including node takeovers, attacks on the routing protocols, and attacks on a node's physical security. In this section, we first address some common denial of service attacks.

A. Types Of Denial Of Service Attacks -The transmission of a radio signal that interferes with the radio frequencies being used by the sensor network is called jamming [5].Jamming may come in two forms: constant jamming, and intermittent jamming. Constant jamming implies the jamming of the entire network. While in the case of intermittent jamming, the sensor nodes are able to exchange messages periodically. At the link layer, one possibility is that an attacker may simply intentionally violate the communication protocol, e.g., ZigBee [17] or IEEE 802.11b protocol, and continually transmit messages in an attempt to generate collisions. Such collisions would require the retransmission of any packet lost by the collision. At the routing layer, a node may take advantage of a multi-hop network by simply refusing to route messages. With the net result being that any neighbor who routes through the malicious node will be unable to exchange messages with the part of the network. The transport layer is also vulnerable to attack, as in the case of flooding[18]. Flooding means sending many connection requests to a malicious node. In this case, resources must be allocated to handle the connection request. Eventually a node's resources will be exhausted, thus rendering the node useless.

B. The Sybil attack - Reference [7] defines Sybil attack as a malicious node illegitimately taking on multiple identities. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-topeer networks.

C. Traffic Analysis- Attacks Often, for an attacker to effectively render the network in useless state, the attacker can simply disable the base station. To make matters worse, Authors in [8] demonstrate two attacks that can identify the base station in a network without even understanding the contents of the packets. A rate monitoring attack posits that nodes close to the base station tend to forward more packets than those farther away from the base station. While in a time correlation attack, an attacker generates events and monitors to whom a node sends its packets.

D. Node Replication- Attacks By copying the node ID of an existing node an attacker can add a node to an existing sensor network. A replicated node can severely disrupt a sensor network's performance; packets can be corrupted or even misrouted. This can result in a disconnected network and false sensor readings [9].

E. Physical Attacks- Indeed, in hostile outdoor environments, the small form factor of the nodes, coupled with the unattended and distributed nature of their deployment makes them vulnerable to physical attacks [10,16].Physical attacks ruin sensors permanently, so the losses are irreversible. For instance, attackers can access cryptographic secrets, tamper with the associated circuitry, spoofing / modifying programming in the nodes, and/or replace them with malicious nodes all of these within the control of the attacker.

III. Counter Measures In Wsn

This section describes the countermeasures for satisfying the security requirements and protecting the sensor network from attacks. B. Defending Against Attacks on Routing Protocols There is a great need for both secure and energy efficient routing protocols in WSNs against attacks such as the sinkhole, wormhole and Sybil attacks. Authors in [15] describe an intrusion tolerant routing protocol, INSENS, which is designed to limit the scope of an intruder ruining and rout information within network intrusion. They posit utilizing the base station to compute routing tables on behalf of the individual sensor nodes[11]. This is done in three phases. The forwarding tables will include the redundancy information used for the redundant message transmission[18]. Attacks that can be made on the routing protocol during each of the three phases above are: First, sensor node might fool the base station by sending a bogus request message. Second, a compromised node might also include a bogus path(s) when forwarding the requested message to its neighbors. Finally, it may not even forward the requested message at all.

C. Combating Traffic Analysis Attacks- Authors in [8] use a random walk forwarding mechanism that occasionally forwards a packet to a node other than the sensor's parent node. This would make it difficult to discern a clear path from the sender node to the base station BS and would help to mitigate the rate monitoring attack, but would still be susceptible to the time correlation attack. To strive against the time correlation attack[14], it suggests a fractal propagation strategy[15]. In this mechanism a node will generate a forged packet when its neighbor is forwarding a packet to the base station. The forged packet is sent randomly to another neighbor who may also generate a forged packet. These packets essentially use a time-to-live to decide when the packet should discard. This effectively hides BS from time correlation attacks.

D. Key Management and Protocols- Sensor nodes may be deployed in a hostile environment; however, security becomes extremely important, as they are prone to variant types of malicious attacks. The open problem is how to set up pair-wise secret key between communicating nodes. In one of the recently presented secure schemes [1,7], the authors describe security as important as performance and energy efficiency for many applications. Key pre-distribution is a good idea to solve the key agreement problems in wireless sensor network, but in this case, the attacker might reveals it after compromising the node.

E. Secure Broadcasting and Multicasting- The major communication pattern of wireless sensor networks is broadcasting and multicasting. The key distribution center is the root of the key hierarchy while individual sensor nodes make up the leaves. By utilizing this technique, they modify the logical key hierarchy to build a directed diffusion based logical key hierarchy. This technique provides mechanisms for sensor nodes joining and leaving groups where the key hierarchy is used to effectively re-key all nodes within the leaving node's hierarchy.

F) Secure Broadcasting Pattern: Reference [7] suggests a routing-aware based tree where the leaf nodes are assigned keys based on all relay nodes above them. This technique takes advantage of routing information and is more energy efficient than mechanisms that arbitrarily arrange sensor nodes into the routing tree.

IV. Conclusions:

WSNs have became promising technology to many applications. In the absence of adequate security, deployment of sensor networks is vulnerable to variety of attacks. In this paper we have outlined the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories we have also sub-categorized the major topics including routing, key management, denial of service, and so on. Our aim is to provide a general overview of the rather broad area of wireless sensor network, security issues, and threat models give the main citations such that further review of the relevant literature can be completed by the interested researcher. As wireless sensor networks continue to grow and become more common need for security in WSN applications will grow even further. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas. On the basis of our observation we motivate the need of a security framework to provide countermeasures against attacks in WSNs.

References:

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Asurvey on sensor etworks,” IEEE Communications Magazine, vol. 40, no. 8, pp.102-114, August 2002.

[2] D. W. Carman, P. S. Krus, and B. J. Matt, “Constraints and approaches for distributed sensor network security,”

Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood,MD, 2000.

[3] HBE-Zigbex. Ubiquitous sensor network. Zigbex Manual. [Online].Available: http://www.hanback.co.kr.

[4] Y. Xiao, “Security in distributed, grid, and pervasive computing,” (Eds.) Chapt.17, in Wireless sensor network security: A Survey, J. P. Walters, Z. Liang,W. Shi, and V. Chaudhary, Auerbach Publications, CRC Press, 2006.

[5] A. D. Wood and J. A. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, 2002

[6] L. K. Bysani and A. K. Turuk, “A Survey on Selective Forwarding Attack in Wireless Sensor Networks,” in 2011 International Conference on Devices and Communications (ICDeCom), Feb., pp. 1–5.

[7] L. Lazos and R. Poovendran, “Secure broadcast in energy-aware wireless sensor networks,” in Proc. IEEE International Symposium on Advances in Wireless Communications (ISWC 02), BC Canada, 2002.

[8] J. Deng, R. Han, and S. Mishra, “Countermeasures against traffic analysis in wireless sensor networks,” Technical ReportCU-CS-987- 04, University of Colorado at Boulder, 2004.

[9] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symposium on Security and Privacy (SSP 05), May 2005, pp. 49-63.

[10] V. Maty_a_s and J. K_ur. Conicts between intrusion detection and privacy mechanisms for wireless sensor networks. IEEE Security and Privacy, 11(5):73-76, 2013.

[11] S. Misra and G. Xue. E_cient anonymity schemes for clustered wireless sensor networks. International Journal of Sensor Networks, 1(1-2):50-63, 2006.

[12] D. Niculescu. Communication paradigms for sensor

networks. IEEE Communications Magazine, 43(3):116-122, 2005.

[13] C. Karlof and D.Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In Proceedings of the 1st IEEE International Workshop on
, 11(5):73-76, 2013.

Sensor Network Protocols and Applications, pages 113-127, 2003.

[14] V. Maty_a_s and J. K_ur. Conicts between intrusion detection and privacy mechanisms for wireless sensor networks. IEEE Security and Privacy