Security Problems in Wireless Sensor Networks – a sketch

[1]K.Ramesh Rao [2]Dr. S.N.Tirumala Rao [3]Prof. P. Chenna Reddy

[1]*Reseacrch Scholor, CSE, , JNTUA , Anantapuramu (A.P)-India,*
[2]*Professor, Dept. of CSE, NarasaraoPeta Engineering College, Narasaraopeta, Guntur (A.P)-India*
[3]*Professor, Dept.of CSE, Director, IRP & SCDE, JNTUA, Anantapuramu(A.P)- India*

Abstract *— A wireless sensor network (WSN) could be a spatially distributed autonomous sensors to watch and hand in glove report data regarding physical or environmental conditions, like temperature, sound, pressure, etc. through the network to a server machine. WSNs area unit typically enforced for collection data from insecure atmosphere. Nearly all security protocols for WSN believe that the invader can do entirely management over a sensor node by method of direct physical access. the looks of sensor networks united of the most technology within the future has display numerous challenges to researchers. The challenges thrown by WSNs area unit distinctive given their delicate design and scant resources. despite the fact that 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*

1. INTRODUCTION

The security problems in wireless sensor network is due to the struggle of what proportion resources is exhausted for security in proportion to the sensor application. the present security perspective for WSNs is on a per-attack basis, that creates associate degree inflexible model leading to poor potency and measurability. Making a security framework providing high flexibility, smart measurability and a redundancy-free security layer for the WSN protocol stack and relies on a resource perspective once deciding security solutions, wherever solutions area unit designed to secure every resource within the WSN atmosphere, instead of defend against attacks.

A. Intrusion Detection System

There are unit several challenges to the safety in wireless sensor network and it's owing to some reasons just like the nature of information transfer of wireless communication, restricted resources of sensor nodes, unattended things wherever sensor nodes may well be liable to physical attack, etc. to reinforce the safety of wireless sensor networks authentication techniques, cryptography techniques is used. These solutions alone will ne'er forestall all potential attacks. therefore a second level of security is Intrusion Detection Systems (IDS) .

B. Secure localization in wireless sensor networks

Ad hoc wireless sensor networks (WSNs) have attracted an excellent deal of attention in recent years for his or her broad potential in each military and civilian operations. The proper operations of the many WSNs consider the data of physical sensor locations. However, most existing localization algorithms developed for WSNs area unit susceptible to attacks in hostile environments. As a result, adversaries will simply subvert the traditional functionalities of location-dependent WSNs by exploiting the weakness of localization algorithms. during this paper, we have a tendency to initial gift a general secure localization theme to shield localization from adversarial attacks. we have a tendency to then propose a mobility-assisted secure localization framework for WSNs.

II. INTRUSION DETECTION AND PRIVACY

Wireless sensor networks typically need to be protected not solely against a lively assailant UN agency tries to disrupt a network operation, however additionally against a passive assailant UN agency tries to induce sensitive data regarding the situation of an exact node or regarding the movement of a half-track object. to handle these problems, we will use associate degree intrusion detection system and a privacy mechanism at the same time. However, each of those typically go along with contradictory aims. A privacy mechanism usually tries to cover a relation between numerous events whereas associate degree intrusion detection system (IDS) tries to link the events up. Here, we have a tendency to initial explore many issues which will seem once each associate degree intrusion detection system and a privacy mechanism area unit used within the network. There area unit issues that may occur once each IDSs and privacy mechanisms area unit used at the same time.

A. Downside causes to IDS

Privacy mechanisms sometimes purposely hide the identity of nodes, assign multiple pseudonyms to one node or use dynamically dynamic pseudonyms. so one node might have totally different pseudonyms for communication with different neighbors and these pseudonyms might amendment in time. Packets sent by the node then contain identifiers that area unit comprehendible solely to the current node and also the supposed recipient. this might cause hassle to associate degree ID since it's unable to link overheard packets with a specific sender or recipient. The IDS will not be able to decide whether or not the claimed anonym of a node is true or not.

An IDS concludes that a specific node is malicious. However, it's going to not be able to mark the node as malicious since it's no appropriate symbol of the node that would be unambiguously understood by different nodes. so it'll have hassle providing different nodes with the knowledge that the

Certain node is malicious. associate degree usual thanks to address this downside is to use the physical location of the malicious node. However, the nodes might solely have some data on the radio radiation strength of the received packets, not on the correct sender location.

An IDS might not be able to notice a Sybil attack since it's legitimate for each node to own multiple identities. associate degree IDS while not extra data isn't able to distinguish between a real identity and a malicious identity either unreal or purloined.

Detection accuracy of associate degree IDS might decrease if it doesn't grasp the identities of its neighbors. as an example, so as to notice a selective forwarding attack associate degree IDS monitors (Node A within the figure two.1) packets in its communication vary. If the IDS overhears a packet (from the node X), it's going to wish to see whether or not the packet is correctly forwarded by the recipient (the node Y). If the IDS assumes that the recipient is in its communication vary, whereas it really isn't, false positives would possibly occur. On the contrary, if the IDS assumes the recipient is out of reach and it's not true, false negatives would possibly occur.

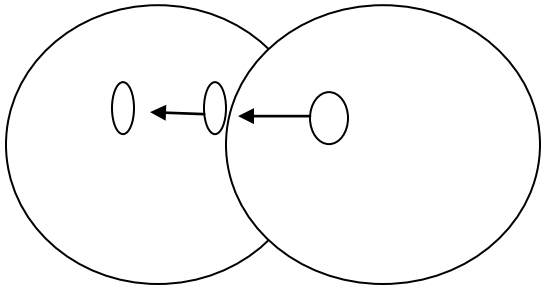

Fig. Communication range between the nodes

An IDS might not be able to notice a selective forwarding (jamming) attack just in case a forwarding (jamming) node has multiple identities and also the IDS doesn't grasp that these identities belong thereto node. Then the IDS cannot link to dropping (sending) events that look innocent once separated associate degreed would be recognized as an attack once joined along. what is more, the IDS must maintain larger tables within the memory owing to a better range of identities monitored.

B. Non-interfering privacy mechanisms

The simplest thanks to avoid all of the said problems is to run protocols that don't cause these issues. However, the possible values for this evasion are a decrease in performance (security functionality) of either IDSs, privacy mechanisms or each. Another impact is a rise in protocol complexness. as an example, the IDS might use a node behavior to spot the node rather than the node symbol. Such behavior could also be described by hashes of messages sent by the node recently. This data is understood by all nodes within the communication vary of the malicious one.

Privacy mechanisms build a large number during a network by activity identities of nodes, introducing new traffic, etc. Privacy mechanisms would possibly share some (secret) data with associate degree IDS, above all ought to this sharing facilitate the IDS to arrange the mess" and with success notice active attackers. a haul to unravel is that an exact IDS node might accumulate plenty of secret data, changing into a sweet spot for associate degree assailant. the subsequent approaches to sharing is taken.

1. Pre-shared secret: Privacy mechanisms uses a trapdoor perform for anonym generation, content protection or dummy traffic identification. The trapdoor data is pre-shared between a privacy mechanism associate degreed an IDS, so the IDS is aware of all the knowledge necessary to run properly.

No more cooperation is required. However, the IDS knowing the trapdoor data is tempting for associate degree assailant. The impact of associate degree IDS compromise is reduced by sharing solely partial data or data that's valid just for an exact time.

2. Delayed data disclosure: bound data is retrospectively discovered by privacy mechanisms, particularly if this data helps the IDS to grasp audit information recorded within the past. This approach assumes that associate degree assailant wants the knowledge straight off and delayed revealing isn't useful for her. This approach is used, as an example, to retrospectively differentiate dummy and real traffic.

3. Data is discovered on demand: the knowledge necessary to cancel the impact of privacy mechanisms' protecting actions is obtained by associate degree IDS on demand, if the IDS executes a further protocol and a privacy mechanism cooperates. The key characteristics area unit that IDSs cannot acquire while not cooperation of privacy mechanisms and also the obtained information is restricted to cancelling effects of privacy mechanism protecting actions just for an exact subject or period.

4. Threshold theme for data availability: data offered to associate degree IDS running on a specific node is purposely restricted to produce extra resilience against the node compromise. to get full data needed, multiple nodes with associate degree IDS/privacy mechanism should work, probably with the support of an acceptable science threshold theme.

C. IDS Leverage

Co-existence of IDSs and privacy mechanisms might profit each once used properly. If associate degree IDS has many identities, it can, as an example, send a searching message (using one identity) that ought to be forwarded back to itself (represented by another identity). These searching messages increase the number of traffic and should play the role of dummy traffic. This additionally makes the traffic analysis more durable and helps the privacy mechanism. Another profit is that associate degree assailant cannot simply avoid associate degree IDS by choosing one (static) path while not IDSs if a privacy mechanism ensures that multiple routes or every which way chosen routes area unit used.

III. ATTACKS ON SENSOR NETWORKS

Wireless sensor networks aren't restricted to easily denial of service attacks, however rather cover a range of techniques together with node takeovers, attacks on the routing protocols, and attacks on a node's physical security. during this section, we have a tendency to initial address some common denial of service attacks .

A. forms of Denial of Service attacks

The transmission of a radio radiation that interferes with the radio frequencies being employed by the sensor network is termed electronic jamming .Jamming might are available in 2 forms: constant electronic jamming, and intermittent electronic jamming. Constant implies the jamming of the complete network. whereas within the case of intermittent electronic jamming, the sensor nodes area unit able to exchange messages sporadically. At the link layer, one risk is that associate degree assailant might merely purposely violate the communication protocol, e.g., ZigBee or IEEE 802.11b protocol, and regularly transmit messages in a trial to get collisions. Such collisions would need the retransmission of any packet lost by the collision. At the routing layer, a node might cash in of a multi-hop network by merely refusing to route messages. With cyber web result being that any neighbor UN agency routes through the malicious node are unable to exchange messages with the a part of the network. The transport layer is additionally susceptible to attack, as within the case of flooding. Flooding suggests that causation several association requests to a malicious node. during this case, resources should be allotted to handle the association request. Eventually a node's resources are exhausted, so rendering the node useless.

B. The Sybil attack

Reference defines Sybil attack as a malicious node illegitimately taking over multiple identities. it had been originally described as associate degree attack able to defeat the redundancy mechanisms of distributed information storage systems in peer-to-peer networks.

C. Traffic Analysis Attacks

Often, for associate degree assailant to effectively render the network in useless state, the assailant will merely disable the bottom station. to create matters worse, Authors in [8] demonstrate 2 attacks which

Layers	Attack Type	Counter Measures
Application Layer	Subversion and malicious nodes	Malicious Node detection and Isolation
Network Layer	Sinkholes, wormholes, Sybil, Routing loop	Key Management, Secure Routing
Data Link Layer	Link Layer Jamming	Link Layer encryption
Physical Layer	DoS and Node capture attack	Adaptive antennas, Spread Spectrum

will determine the bottom station during a network while not even understanding the contents of the packets. A rate observation attack posits that nodes near the bottom station tend to forward additional packets than those further far away from the bottom station. whereas during a time correlation attack, associate degree assailant generates events and monitors to whom a node sends its packets.

D. Node Replication Attacks

By repetition the node ID of associate degree existing node associate degree assailant will add a node to associate degree existing sensor network. A replicated node will severely disrupt a sensor network's performance; packets is corrupted or perhaps misrouted. this could end in a disconnected network and false sensor readings .

E. Physical Attacks

Indeed, in hostile outside environments, the tiny kind issue of the nodes, as well as the unattended and distributed nature of their readying makes them susceptible to physical attacks Physical attacks ruin sensors for good, therefore the losses area unit irreversible. as an example, attackers will access science secrets, tamper with the associated electronic equipment, spoofing / modifying programming within the nodes, and/or replace them with malicious nodes all of those at intervals the management of the assailant.

IV. COUNTER MEASURES IN WSN

This section describes the countermeasures for satisfying the safety needs and protective the sensor network from attacks. Table I below summarizes the attacks and counter-measures during a layering model in WSNs

A. defensive Against DoS Attacks

One strategy in defensive against the electronic jamming attack is to spot the crowded a part of the sensor network and effectively route round the untouchable portion. To handle electronic jamming at the waterproof layer, nodes would possibly utilize a waterproof admission management that's rate limiting. this may permit the network to ignore those requests designed to exhaust the facility reserves of a node. This, however, isn't fool-proof because the network should be able to handle any lawfully massive traffic volumes.

B. defensive Against Attacks on Routing Protocols

There is an excellent would like for each secure and energy economical routing protocols in WSNs against attacks like the natural depression, hollow and Sybil attacks. Authors in describe associate degree intrusion tolerant routing protocol, INSENS, that is meant to limit the scope of associate degree persona non grata ruin and rout data at intervals network intrusion. They posit utilizing the bottom station to calculate routing tables on behalf of the individual sensor nodes. this can be wiped out 3 phases. The forwarding tables can embody the redundancy data used for the redundant message transmission. Attacks which will be created on the routing protocol throughout every of the 3 phases higher than are: initial, sensor node would possibly fool the bottom station by causation a counter feit request message. Second, a compromised node may also embody a counter feit path(s) once forwarding the requested message to its neighbors. Finally, it's going to not even forward the requested message in the slightest degree.

C. Prevent Traffic Analysis Attacks

Authors in use a stochastic process forwarding mechanism that sometimes forwards a packet to a node aside from the sensor's parent node. this may build it troublesome to pick out a transparent path from the sender node to the bottom station SB and would facilitate to mitigate the speed observation attack, however would still be liable to the time correlation attack. To attack the time correlation attack, it suggests a shape propagation strategy .In this mechanism a node can generate a solid packet once its neighbor is forwarding a packet to the bottom station. packet is shipped every which way to a different neighbor UN agency might also generate a

forged packet. These packets primarily use a time-to-live to choose once the packet ought to discard. This effectively hides SB from time correlation attacks.

D. Key Management and Protocols

Sensor nodes could also be deployed during a hostile environment; but, security becomes very vital, as they're at risk of variant forms of malicious attacks. The open downside is a way to created pair-wise secret key between communication nodes. In one in all the recently bestowed secure schemes , the authors describe security as vital as performance and energy potency for several applications. Key pre-distribution could be a smart plan to unravel the key agreement issues in wireless sensor network, however during this case, the assailant would possibly reveals it when compromising the node. supported the Key-Insulated Encryption(KIE)-WSNs, authors have projected a replacement key pre-distribution theme. They achieved each semantically security and optimum KIE-(N-1, N) safety, which implies that though N-1 nodes area unit compromised, there are not any security threat to the remaining network.

E. Secure Broadcasting and Multicasting

The major communication pattern of wireless sensor networks is broadcasting and multicasting,

1) Secure Multicasting Pattern: Reference proposes a directed diffusion primarily based multicast technique for wireless sensor networks considering .

2). Also the advantage of a logical key hierarchy. The key distribution center is that the root of the key hierarchy whereas individual sensor nodes conjure the leaves. By utilizing this method, they modify the logical key hierarchy to make a directed diffusion primarily based logical key hierarchy. this method provides mechanisms for sensor nodes change of integrity and departure teams wherever the key hierarchy is employed to effectively re-key all nodes at intervals the departure node's hierarchy.

3). Secure Broadcasting Pattern: Reference suggests a routing-aware primarily based tree wherever the leaf nodes area unit appointed keys supported all relay nodes higher than them. this method takes advantage of routing data and is additional energy economical than mechanisms that haphazardly prepare sensor nodes into the routing tree.

V. CONCLUSION

WSNs have became promising technology to several applications. With in the absence of adequate security, readying of sensor networks is susceptible to type of attacks. during this paper we've made public the four main aspects of wireless sensor network security: obstacles, needs, attacks, and defenses. at intervals every of these classes we've additionally sub-categorized the key topics together with routing, key management, denial of service, and so on. Our aim is to produce a general summary of the rather broad space of wireless sensor network, security problems, and threat models provide the most citations such more review of the relevant literature is completed by the interested man of science.

As wireless sensor networks still grow and become additional common would like for security in WSN applications can grow even more. we have a tendency to additionally expect that the present and future add privacy and trust can build wireless sensor networks a additional engaging choice during a type of new arenas. On the premise of our observation we have a tendency to inspire the necessity of a security framework to produce countermeasures against attacks in WSNs.

VI REFERENCES

[1] Kahina CHELLI “Security Issues in Wireless Sensor Networks: Attacks and Countermeasures” Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1 - 3, 2015, London, U.K.

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

[3] 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.

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

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] D. Niculescu. Communication paradigms for sensor networks. IEEE Communications Magazine, 43(3):116-122, 2005.

[14] C. Karlof and D.Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, pages 113-127, 2003.

[15] 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. Sujesh P. Lal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 920-924 www.ijcsit.com 923

[16] F. Liu, X. Cheng, and D. Chen. Insider attacker detection in wireless sensor networks. In Proceedings of the 26th IEEE International Conference on Computer Communications, pages 1937{1945, 2007.

[17] A. Stetsko, L. Folkman, and V. Matyas. Neighbor-based intrusion detection for wireless sensor networks. Technical Report FIMU-RS-2010-04, Faculty of Informatics, Masaryk University, May 2010.

[18] Wireless Ad Hoc and Sensor Networks. [Online]. Available: http://www.zigbee.org/ 2005.

[19] Sujesh P Lal, Prof. H R Viswakarma. QoS Based Bandwidth Allocation for Networks. Volume-2, Number-2, December 2009. Pages 111-119.

[20] M. Cinque, A. Coronato, A. Testa, and C. Di Martino, "A Survey on Resiliency Assessment Techniques for Wireless sensor Networks," in Proceedings of the 11th ACM International Symposium on Mobility Management and Wireless Access, New York, NY, USA, 2013, pp. 73–80.