International Journal of Security and Its Applications
Vol. 12, No. 5 (2018), pp.1-10
http://dx.doi.org/10.14257/ijsia.2018.12.5.01

Security Issues and Attacks in Wireless Sensor Networks: Some Case Studies

N. Thirupathi Rao[1], Debnath Bhattacharyya[1] and Tai-Hoon Kim[2*]

[1]*Department of Computer Science & Engineering*
Vignan's Institute of Information Technology (A)
Visakhapatnam, AP, India
[3]*Sungshin Women's University, Bomun-ro 34da-gil, Seongbuk-gu, Seoul, Korea*
nakkathiru@gmail.com, debnathb@gmail.com, taihoonn@daum.net

Abstract

Remote sensor arranges is a standout amongst the most developing innovation for detecting and playing out the distinctive undertakings. Such systems are valuable in numerous fields, for example, crises, wellbeing observing, ecological control, military, ventures and these systems inclined to malignant clients' and physical assaults because of radio scope of system, un-put stock in transmission, unattended nature and get to effectively. Security is a crucial necessity for these systems. In this paper, our focal point of consideration is on physical assaults and issues in remote sensor systems. Through this audit, effectively distinguish the reason and abilities of the aggressors. Further, we talk about understood methodologies of security discovery against physical assaults.

Key words: *Physical attacks, Wireless sensor network, Security*

1. Introduction

The security of system is a major issue for security executives since organize is developing step by step. Security on the Internet and on Local Area Networks is currently at the bleeding edge of PC organize related issues [1]. The alluring highlights of systems, for example, open medium, dynamic topology, nonattendance of focal experts, and disseminated participation hold the guarantee of altering the specially appointed systems over a scope of common, logical, military and modern applications. Nonetheless, these attributes make MANET systems powerless against various sorts of assaults and make executing security in specially appointed system a testing assignment. The fundamental security issues that should be managed in MANET systems include: verified gadgets, the protected directing in multi-bounce systems, and the safe exchange of information. This implies the collector ought to have the capacity to affirm that the personality of the source or the sender (*i.e.*, one bounce past hub) is for sure who or what it cases to be. It likewise implies that the collector ought to have the capacity to check that the substance of a message has not been changed either malignantly or incidentally in travel.

Remote Manet is another foundation less correspondence innovation which is comprises of those conditions where administration of framework costs high. Aside from this legitimacy it has bad marks as far as secure correspondence. Manet is characterized by its highlights like self sorting out, circulated application and multi hub steering. Because of its dynamic nature keeping up the secured correspondence is monotonous when brought together administration does not exist. In such condition key administration plans is a troublesome assignment to accomplish a protected correspondence. Utilizing overseeing of secure key dissemination for security speed fluctuates with respect to the

Received (January 5, 2018), Review Result (April 16, 2018), Accepted (April 21, 2018)
* Corresponding Author

ISSN: 1738-9976 IJSIA

applications. For instance, in military based application it will require ling investment because of long range organize yet in business applications it will require a short investment because of short separation. So we can state speed is contrarily relative to arrange go. In key administration plans distinctive cryptographic keys technique are utilized like symmetric keys, open keys or authentication based cryptography.

In this approach both the sender and the beneficiary contains a similar key for encryption and for unscrambling. Out in the open key encryption two keys are utilized one private key and alternate as open key. The private keys are utilized for encryption between the hubs though open keys are utilized for encryption. Their plans rely upon testament based cryptography (CBC) where the authentication issue expert uses ID based cryptography to create the declaration. Gary C. Kessler has proposed this plan in his work for secured correspondence. Other is Identity based cryptography. In this plan an openly known key is speaking to an association and utilized as open key. The functional execution of this plan is finished by Sakai in 2000.

2. Related Works

A versatile impromptu system (MANET) is a remote correspondence arranges which does not depend on a prior framework or any brought together administration. Securing the trades in MANETs is necessary to ensure a far reaching improvement of administrations for this sort of systems. The organization of any security strategy requires the meaning of a trust display that characterizes who puts stock in who and how. Our work expects to give a completely circulated trust show for portable specially appointed systems. In this paper, we propose a completely disseminated open key testament administration framework in view of confide in charts and limit cryptography. It licenses clients to issue open key declarations, and to perform validation by means of endorsements' chains with no brought together administration or trusted experts [1].

The trust is constantly present certainly in the conventions in light of collaboration, specifically, between the 26 substances associated with steering activities in Ad hoc arranges. In reality, as the remote scope of such hubs 27 is restricted, the hubs commonly participate with their neighbors to expand the remote hubs and 28 the whole system [2]. A portable impromptu system (MANET) alludes to a system intended for extraordinary applications for which it is hard to utilize a spine organize. In MANETs, applications are for the most part required with touchy and mystery data. Since MANET expects a trusted domain for steering, security is a noteworthy issue [3]. Enhanced Link State Routing is a steering convention that has been broadly considered for portable specially appointed systems. Connection mocking, which aggravates the directing administration, is one of the basic security issues identified with the OLSR convention.

Existing methodologies against interface caricaturing assault have a few downsides. In this paper, propose a LT-OLSR convention that communicates Hello messages to neighbors inside two-bounces to safeguard systems against connect mocking assaults [4]. Versatile Ad hoc arrange is comprises of portable hubs and can sort out them self without requiring any framework. Because of remote correspondence any hub can join or leave organize which causes part of security requirement and because of constrained battery numerous scientists are doing explores on vitality sparing steering in MANET. In OLSR there is need of choosing MPR set, which limit pointless communicate in arrange, that monitor vitality of hub in organize [5]. Two measures to counter assaults against OLSR: counteractive action that settles some convention's vulnerabilities and countermeasures that treat misconduct and irregularity worried by the vulnerabilities that have not been comprehended with aversion measures. The subsequent instruments permit settling the OLSR vulnerabilities which are because of the simple usurpation of hub's personality, and the absence of connections check at the area disclosure [6].

Agreement Attack is an assault against Mobile Ad Hoc Networks and depends on Optimized Link State Routing (OLSR) Protocol. In this assault, two assaulting hubs intrigue to forestall courses to an objective hub from being set up in the system. Parcel Delivery Ratio (PDR) of hubs 2-jumps from the casualty drops to 0%. Multi Point Relay (MPR) choice process in OLSR is misused to accomplish course dissent. In this paper, propose a novel assault safe technique named Forced MPR Switching OLSR (FMS-OLSR), in which, at whatever point a hub watches indications of the assault, it incidentally boycotts potential assailants [7]. Portable specially appointed systems (MANETs) are outstanding to be helpless against different assaults because of their absence of concentrated control, and their dynamic topology and vitality obliged activity. Much research in securing MANETs has concentrated on propositions which distinguishes and keep a particular sort of assault, for example, lack of sleep, dark opening, dim gap, surging or sybil assaults. In this paper propose a summed up interruption recognition and avoidance instrument. We utilize a blend of oddity based and learning based interruption discovery to secure MANETs from a wide assortment of assaults [8].

Portable specially appointed systems are defenseless against an assortment of system layer assaults, for example, dark gap, dim opening, lack of sleep and surging assaults. In this paper we show an interruption discovery and versatile reaction instrument for MANETs that recognizes a scope of assaults and furnishes a viable reaction with low system debasement. We think about the insufficiencies of a settled reaction to an interruption; and we beat these lacks with an adaptable reaction plot that relies upon the deliberate trust in the assault, the seriousness of assault and the corruption in arrange execution [9]. Notwithstanding, MANETs are helpless against different assaults at all layers, incorporating into specific the system layer, in light of the fact that the plan of most MANET steering conventions expect that there is no pernicious interloper hub in the system [10]. OLSR depends on the collaboration between organize hubs, it is defenseless to a couple of conniving maverick hubs, and at times even a solitary malevolent hub can cause steering.

There are some different choices that work pleasantly within the sight of one traded off hub, however the adequacy is lost when numerous assailants that are conniving. For finding the noxious node(s) a novel technique has been proposed by Sakshi Jain and Ajay Khuteta [6]. Their strategy depends on Base Node (BN) sending sham RREQ parcel at each time interim. Typical hubs don't send answer as the sham RREQ is for hub that don't exist in organize. Just noxious hubs will send an answer since they don't check in their table for course to goal and begin producing course answer message. BN hub in this manner identifies that noxious hub and offers it with all the ordinary hubs for hindering the correspondence to and from these vindictive hubs. This system incredibly decreases the likelihood of dark gap assault in arrange and furthermore lessens vitality and postponement in MANETs. Utilizing comparable idea Farrukh Aslam Khan *et.al.*, [7] have composed a location and avoidance framework (DPS) against community oriented assault in MANETs. In their proposed strategy, all transmitted RREQs bundle are routinely checking by extra node(s) (DPS Nodes) in the system. After investigation DPS Node(s) distinguish suspicious node(s) and communicate piece message for these noxious hubs to the system.

An alternate approach is utilized by Dhiraj Nitnaware and Anita Thakur [8]. Creators have outlined DYMO-AODV convention in view of BDS system; that changes the AODV convention. In this approach there are three stages are Broadcast Hello parcel, Suspicious Node Detection and Suspicious Node Prevention. Every last hub gets communicated hi parcel and procedures the capacity check of each versatile hub. Here, Hello bundle shrouds the discovery system which gathers the equipment data of current hub and confirms this with edge esteem. On the off chance that any hub is seen with

additional conventional capacity it is considered as the noxious hub and this data is sent to aversion component.

Utilizing fairly comparable strategy Nitika Gupta and Shailendra Narayan singh [9] proposed an advanced mark procedure to keep the wormhole assault in systems. Group head (CH) and Cluster door (CG) keep up the correspondence between the hubs or two bunches by utilizing open keys verification strategy. The proposed convention is keeping the wormhole assault with cryptography idea however without utilizing any mind boggling equipment execution.

H. Vignesh Ramamoorthy and Dr. D. Suganya Devi [10] have proposed a strong approach utilizing few control bundles to perceive a moderately ideal way for routing. A substitute course is pre-registered for any course disappointment amid information exchange. The suggested conspire is multi operator subterranean insect based steering which has joined the element of proactive and receptive idea in one directing convention. The proposed half and half steering convention give better execution in adaptability highlight and network of hubs. The offered incorporated approach has additionally a limited the conclusion to-end postpone and the course revelation inactivity.

Partha Sarathi Banerjee et.al.[11] have proposed trust based AODV steering convention that works with three fluffy rationale based participation capacities PI-enrollment work, Gaussian participation work and Triangular-participation work for trust esteem count utilizing multi criteria to distinguish untrusted neighbors. Just trusted neighbors are utilized for bundle exchanges. Creators have displayed an approach that yields better throughput without narrow minded hub. Key focal point of the plan is to send bundles over a remote medium with vitality proficient and invalidated of malignant hub.

Tarunpreet Bhatia and A.K. Verma [12] have featured the Black gap assault impact on AODV directing in MANRT and gave an answer for conquering the pernicious impact. Creators break down the distinctive situations under different parameters to assess the harms caused to the system. They gave proficient security capacities to apply ton AODV convention as answer for beat dark opening assaults. The reenactment reports demonstrate that event of black hole hubs will cause an unfavorable impact on the AODV execution like bundle conveyance portion, number of dropped parcels, throughput and standardized directing burden.

3. Security Assaults

Security assaults can be grouped under the accompanying classes:

3.1. Inactive assaults.

This kind of assaults incorporates endeavors to break the framework by utilizing watched information. One of the case of the inactive assault [8,11] is plain content assaults, where both plain content and figure content are as of now known to the aggressor.

The traits of detached assaults are as per the following:

1. **Interception:** assaults classification, for example, listening stealthily, "man-in-the-center" assaults.
2. **Traffic Analysis:** Assaults classification, or obscurity. It can incorporate follow back on a system, CRT radiation.

3.2. Dynamic Attacks

This kind of assault requires the assailant to send information to either of the gatherings, or piece the information stream in one or on the other hand the two bearings. [8, 11] The traits of dynamic assaults are as per the following,

1. **Interruption:** Assaults accessibility, for example, foreswearing of-benefit assaults.
2. **Modification:** Assaults respectability.
3. **Fabrication:** Assaults credibility.

4. System Safety Events.

The following are the several measures to be followed or to be considered as follows [6]:

- A solid firewall and intermediary to be utilized to keep undesirable individuals out.
- A solid Antivirus programming bundle and internet safety software bundle ought to be introduced.
- For validation, utilize solid passwords and change it on a week by week/fortnightly premise.
- Employees ought to be careful about physical security.
- Prepare a system analyzer or system screen and utilize it when required.
- Implementation of physical safety efforts like shut circuit TV for section regions and confined zones.
- Security hindrances to confine the association's border.
- Fire asphyxiators can be utilized for flame touchy territories like server rooms and security rooms.

5. System Security Tools.

Following apparatuses are utilized to secure the system [4]:

- N-outline Scanner is a free and open source utility for organize investigation or security examining.
- Nessus is the best free system helplessness scanner accessible.
- Wire shark or Ethereal is an open source arranges convention analyzer for UNIX and Windows.
- Kismet is an intense remote sniffe

6. Secure Neighbor Discovery

In remote systems, every hub has to know its neighbors to settle on directing choices; it stores neighbor data in its steering table that contains the address of the neighbor, and the connection state. In MANETs, hubs utilize neighbor disclosure convention to find encompassing hubs they can specifically speak with over the remote channel with flag proliferation speed by thinking about the area or round trek data.

6.1. Secure Routing Packets.

Once accomplish secure data trade, we can additionally secure the basic directing convention in remote specially appointed systems. Security benefits in MANETs have a place with two sorts of back rubs: the directing back rubs and the information messages.

Both have an alternate nature and diverse security needs. We center here around securing steering since information messages are point-to-point and can be ensured with any point-to-point security framework. Then again, steering messages are sent to moderate neighbors, handled, perhaps altered, and despise. Also, because of preparing of directing message, a hub may adjust its steering table. This makes the requirement for both the conclusion to-end and the middle hubs to have the capacity to verify the data contained in the steering messages.

6.2. Fundamental Types of Attacks

Here we are showing some fundamental class of assaults which can be a reason for moderate system execution, uncontrolled movement, infections and so forth.

A. Security Hazard

There are various security dangers that can be the reason for a system security assault. Principle security dangers are foreswearing of administration, disseminated disavowal of administration, infections, Trojan steeds, spywares, malwares, unapproved access to the system assets and information, incidental cancellation of the documents and the uncontrolled web get to.

B. Infection Assault

A PC contamination is a little program or an executable code that when executed and replicated, perform assorted unwanted and dangerous capacities with regards to a PC and a framework. Diseases can wreck your hard plates and processors, exhaust memory at an enormous scale and demolish the general execution of a PC or framework. A Trojan is a malicious code that performs dangerous exercises anyway it can't be repeated. Trojan can squash structures' essential data. A PC worm is a program that copies to all framework and pulverize profitable data. The diseases, malware, adware and Trojan steeds can be checked if you have a revived antivirus program with the latest illustration reports.

C. Unapproved Contact

Access to the system assets and information ought to be enabled just to the approved people. Each common organizer and assets in your system ought to have been gotten too just by the approved people and ought to likewise be checked and observed consistently.

D. Data Robbery and Cryptography Assaults

Another risk to a system is to loss of the essential data and this misfortune can be averted, on the off chance that you great encryption strategies, for example, 128 piece security or 256 piece security encryption techniques. Along these lines, your information when exchanged through FTP programs, can be scrambled and can't be perused or utilize.

E. Unapproved application establishments

Another infection and security assault avoidance strategy is to introduce just the approved programming applications to our system server and your everything customer PCs. No one ought to be permitted to introduce any sort of program which can cause security dangers, for example, melodies or video programs, codec, gaming programming or other online applications.

6.3. Key Management Scheme

Different key administration plans have been proposed utilizing the quantity of circulation strategies. Different Symmetric key administration plans like Key Infection,

Peer middle of the road key foundation. A portion of the Asymmetric key administration plans are secure steering convention, Ubiquitous and hearty Access yet these plans incorporates the parameters like

- **Increasing Security:** Reducing little estimations will devour less calculation hub energy to enhance arrange security.

- **Expanding Mobility:** Computational strategies can be diminished by diminishing the distribution of assets to broaden versatility.

- **Reducing Key Age Time:** Network quality can be enhanced if key age time can be diminished.

- **Reducing Power:** Due to the battery depended arrange, control protection is critical to enhance the system consistency.

6.4. Essential Defense Instructions.

The fundamental system safety significant safety tips and procedures to secure your framework, for instance, presenting an invigorate antivirus program, email separating programs, sort out checking devices, web get to course of action and other security shirking methodologies. Framework security is the most basic portion in information security since it is accountable for protecting all data experienced sorted out PCs [4, 5]. There are bundle of security endeavors and repugnance strategies which I will discuss around there. Usually a PC framework can be struck by different courses. As often as possible check all the framework devices, messages, open ports, server and client PCs. It's the commitment of the framework officials to check and pass on the missing security settles in the entire framework PCs. They should in like manner clear the pointless framework shares, customer's records, remote access shows and restrains the passageway the framework customers.

A. Kill Ping Examine

The main role of a ping demand is to distinguish has that are presently dynamic. All things considered, it is regularly utilized as a component of observation action going before a bigger, more organized assault. By evacuating a remote client's capacity to get a reaction from a ping demand, you will probably be ignored by unattended sweeps or from "content kiddies," who for the most part will search for a simpler target. Note this does not really shield you from an assault, but rather will make you far more averse to end up an objective. For handicap ping outside from your open IP: for that, the icmpconfig would be the accompanying:

icmp deny any resound outside

icmp allow any outside

reverberate demands get dropped,

be that as it may, the various icmp writes are still permitted.

B. Close unused ports

Ports let the outside world speak with your PC. Think about a port as an entryway: when the entryway is open, anybody can get inside. A shut port guards your PC from

undesirable outside correspondence. In security speech, the term open port is utilized to mean a TCP or UDP port number that is designed to acknowledge parcels. There are different ports and most extreme are as a matter of course open in our PC like FTP, TELNET, UDP, SMTP, FTP and so on. As a rule we require just some port like FTP, HTTP and so on. On the off chance that somebody needs to enter in our system or framework they utilized these sorts of open ports. So if redundant close unused ports. Malignant programmers (or wafers) generally utilize port examining programming to discover which ports are "open" (unfiltered) in a given PC, and regardless of whether a real administration is tuning in on that port. Interestingly, a port which rejects associations or disregards all bundles coordinated at it is known as a "shut port" [6]. Ports can be "shut" using a firewall.

C. Tie IP to MAC Address.

We realize that MAC address is one of a kind number which can't be changed. We can influence a rundown of IP to address utilized as a part of our system and after that predicament those IP delivers to the specific frameworks MAC address. In the wake of doing this action nobody can use out sider framework or workstation in your framework.

D. Utilize Interruption Discovery System and Interruption Avoidance Systems (IPS).

An interruption recognition framework (IDS) reviews all inbound and outbound system action and distinguishes doubtful examples that may demonstrate a system or framework assault by somebody endeavoring to break into or trade off a framework. IDSs utilize activity examination and propelled calculations to decide whether a test has been directed. Numerous IDSs are intended to address expanded prerequisites for security perceivability, disavowal of - benefit (DoS) insurance, hostile to hacking recognition, and e - trade business safeguards. An Interruption Avoidance System (IPS) can take crafted by the IDS above and beyond, by making quick move that does not require human mediation, as IDS alerts are created in light of a predefined set of principles.

7. Security Management Issues

- Ensuring the security quality of the association is a major test these days. Associations have a few
- Pre-characterized security strategies and techniques yet they are not actualizing it in like manner. Using innovation, we ought to force these strategies on individuals and process.
- Building and avowing great assets for sending and proficient administration of system security foundation.
- Adopting advancements that are simple and financially savvy to convey and oversee day-to– day arrange security tasks and investigates over the long haul.
- Ensuring a completely secure systems administration condition without corruption in the execution of business applications.
- On an everyday premise, ventures confront the test of scaling up their foundation to a quickly expanding client gathering, both from inside and outside of the associations. In the meantime, they additionally need to guarantee that execution isn't bargained.
- Organizations now and then need to manage various point items in the system. Securing every one of them absolutely while guaranteeing consistent usefulness is one of the greatest difficulties they confront while arranging and executing a security outline.

System Security cuts over all capacities and subsequently activity and comprehension at the best level is basic. Security is likewise critical at the grassroots level and to

guarantee this, worker mindfulness is a major concern. Being refreshing about the different alternatives and the divided market is a test for all IT chiefs. In the security space, the operational stage accepts a greater significance. Consistence likewise assumes a dynamic part in security; henceforth the business improvement group, fund, and the CEO's office need to grid with IT to convey a diagram.

8. Conclusion

There are different ways, which guarantee for the prosperity and security of your framework. Perform ordinary framework security testing. Do whatever it takes not to give progressively or bothersome access to any framework customer. The networks should have revived an antivirus program. Working structure should be routinely invigorated. In case you have windows based working structure you can revive it from the Microsoft site. Keep load of your framework resources, for instance, contraptions and programming applications. Murder your PC when you are away and don't remove your PC unattended. Put a strong framework and structure executive mystery word. Use a traded framework, with the objective that you can recognize the issue quickly.

References

[1] T. Akin, “Hardening Cisco Routers”, O’Reilly & Associates, **(2002)**.
[2] A. Simmonds, P. Sandilands and L. van Ekert, “Ontology for Network Security Attacks”, Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, **(2004)**, pp. 317-323.
[3] J. Kim, K. Lee and C. Lee, “Design and Implementation of Integrated Security Engine for Secure Networking”, In Proceedings International Conference on Advanced Communication Technology, **(2004)**.
[4] S. Chen, R. Iyer and K. Whisnant, “Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors”, In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., **(2002)**.
[5] H. Kim, “Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System”, IEEE Transactions on Consumer Electronics, vol. 50, no. 1, **(2004)** February.
[6] R. S. Vandana, “Network Security: Attacks, Tools and Techniques”, International Journal of scientific research and management, vol. 3, no. 5, **(2015)**.
[7] M. Omar, Y. Challal and A. Bouabdallah, “Reliable and fully distributed trust model for mobile ad hoc networks”, Computers & Security, vol. 28, **(2009)**, pp. 199-214.
[8] A. Adnane, C. Bidan and R. T. de Sousa Júnior, “Trust-based security for the olsr routing protocol”, Computer Communications, vol. 36, no. 10, **(2013)**, pp. 1159-1171.
[9] M. Marimuthu and I. Krishnamurthi, “Enhanced olsr for defense against dos attack in ad hoc networks”, Journal of Communications and Networks, vol. 15, no. 1, **(2013)** February, pp. 31-37.
[10] Y. Jeon, T.-H. Kim, Y. Kim and J. Kim, “Lt-olsr: Attack-tolerant olsr against link spoofing”, Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks (LCN 2012), ser. LCN ’12. Washington, DC, USA: IEEE Computer Society, **(2012)**, pp. 216-219.
[11] D. Malik, K. Mahajan and M. Rizvi, “Security for node isolation attack on olsr by modifying mpr selection process”, Networks Soft Computing (ICNSC), 2014 First International Conference, **(2014)** August, pp. 102-106.

