International Journal of Advanced Information Science and Technology (IJAIST) *ISSN: 2319:2682*
Vol.5, No.1, January 2016 DOI:10.15693/ijaist/2016.v5i1.77-82

INVESTIGATIONS ON SECURE ROUTING ISSUES IN WIRELESS SENSOR NETWORKS

Ram Pradheep Manohar
Research Scholar
St. Peter'sUniversity, Chennai, India

Dr.E.Baburaj
Professor, Sun College of Engineering and Technology, Nagercoil, India

***Abstract* - As wireless sensor systems keep on developing, so does the requirement for effective security systems. Since sensor systems might cooperate with touchy information and/or work in threatening unattended situations, it is basic that these security concerns be tended to from the earliest starting point of the framework outline. Nonetheless, because of innate asset and figuring imperatives, security in sensor systems postures different challenges than customary system/PC security. There is presently colossal research potential in the field of wireless sensor system security. In this way, recognition with the current research in this field will benefit analysts enormously. In view of this, we review the significant themes in wireless sensor system security, and present the deterrents and the necessities in the sensor security, characterize a large portion of the present attacks, and finally list their comparing guard and presented some future research directions.**

***Keywords:*cryptography; security; attacks; counter attacks; security threats, wireless sensor networks**

1. INTRODUCTION

The requirement for secure routing in Wireless Sensor Networks (WSNs) emerges from the late achievement of WSNs with a specific end goal to give minimal effort/high-advantage situational mindfulness yet the absence of an all-encompassing routing answer for incorporate WSNs into the military particular security principles. In this way there is a colossal measure of progressing exploration in WSNs including the routing parts of it. Subsequent to the nodes of WSNs are extremely restricted, particularly as far as force, the majority of the routing endeavors have concentrated on giving vitality effective arrangements [17]. Notwithstanding, to incorporate WSNs into military's system driven operations, WSNs need to adjust to the military particular security necessities. Along these lines any answer for routing in WSNs ought to consider security as one of the top needs, to which WSN research group hasn't gave careful consideration contrasted with those of vitality productivity [25]. Wireless systems are more inclined to security vulnerabilities because of their show nature, and WSNs, which are involved modest constrained sensor nodes, are much more inclined to security attacks Along these lines the security answers for a workstation then again notwithstanding for a PDA, for instance running a firewall project, are not achievable for WSNs: new approaches and new ideas are required. The general arrangement of Wireless Sensor Networks is shown in Fig.1.

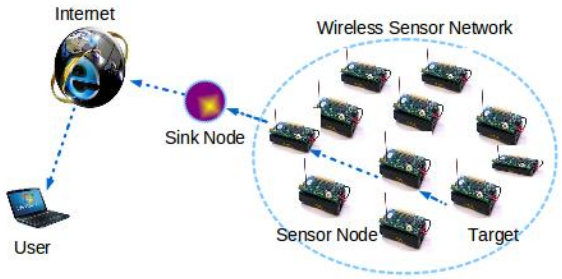

Fig. 1 Wireless Sensor Networks

2. SECURITY REQUIREMENTS

The fundamental point of security parts of WSN is to ensure WSN assets and data. This can be accomplished by satisfying the accompanying security prerequisites. The status of the existing counter attack techniques are not up to the level of meeting the security requirements mentioned in the following section.

2.1. Confidentiality

Privacy is the real sympathy toward accomplishing security in WSN [8][3]. Asset privacy takes a shot at the rule that, "the asset bound for the destination just". In different words a WSN node ought not to spill data about the detected sign at any expense. While transmitting information the sensor node must make a protected channel for the destination.

2.2. Integrity

Classification doesn't mean respectability of information [8]. In spite of the fact that the gatecrasher will most likely be unable to take information however it might change the information in specific cases. Thus the sensor system gets the changed data. Hence Data respectability guarantees that the got information by a node ought to not be modified.

2.3. Freshness

In this prerequisite a node must guarantee that it got the crisp information. Information freshness proposes that the information is later, and it guarantees that no old messages have been despise [9][4].

2.4. Availability

The sensors and the sensor system itself is a rare asset. The accessibility of these assets is key [8][23]. The accessibility of a sensor and sensor system is a dull, on

the grounds that in a WSN extra calculation expends more vitality. So for a safe WSN these assets must be accessible.

2.5. Self-Organization

Like adhoc wireless system a WSN should act naturally sorting out in nature in various situations [5]. For instance if there should be an occurrence of a node disappointment the other stable node must ready to recognize the best way to the destination by bypassing the fizzled node.

2.6. Time Synchronization

Time synchronization is a crucial situation in WSN [6]. Amid transmission the sensor might off or on with a specific end goal to protect vitality. In such a situation it is extremely repetitive to be synchronized. So the sensor node must guarantee that time synchronization is accomplished in such a circulated domain.

2.7. Authentication

Amid information transmission it is prime objective that the information which is proposed for the destination must be conveyed to the destination just. At the end of the day, information validation permits a collector to confirm that the information truly is sent by the asserted sender [10][13]. This can be accomplished by presenting a message validation code (MAC) of all imparted information [3].

2.8. Authorization

Node approval is another viewpoint for giving security in a WSN domain [18]. In this process the collector on gets the information of bona fide senders.

2.9 Strength and Survivability

The sensor system ought to be powerful against different security attacks, and if an attack succeeds, its effect ought to be minimized. The tradeoff of a solitary node ought not break the security of the whole system.

3. THREATS

Numerous sensor system routing conventions are quite basic, and consequently are now and then Defenseless to attacks from the writing on routing in specially appointed systems. Most system layer attacks against sensor systems can be categorized as one of the accompanying classifications:

3.1 Denial of Services Attack

In a WSN, be that as it may, general intelligent registering offices are not prone to exist in any of the devices. The huge number of devices, their relative detachment, and low vitality supplies are more reasonable when confined self-governance what's more, coordination are available. In such a situation, in-system administrations, (for example, limitation, routing, what's more, power administration) are of more straightforward advantage to the sensor nodes that cooperate with them than to the human administrators [20]. As opposed to treat just the human deployers, proprietors, or screens of the system as clients, it might be more valuable to consider individual sensor nodes as clients as for in-system administrations.

A specific trouble on the Internet is that the system is incomprehensible and open, such that it is at present unrealistic to confirm each client. For a few administrations, then, there are successfully no unapproved clients, since clients are most certainly not emphatically validated by any stretch of the imagination.

3.2 Sybil Attack

A Sybil attack is an attack which makes different personalities from same vindictive node. This attack is exceptionally defenseless against wireless sensor system since this nature could be passage of whatever other attacks, for example, wormhole, sinkhole, specific sending and so on… The Sybil attack was acquainted by Douccer in companion with associate system, this attack makes additionally undermining issues in appropriated stockpiling, voting and asset distribution, same as showed up in wireless sensor system, and this was additionally recognized by creator Douccer. Be that as it may, because of their impediment of sensor node, couldn't specifically execute the conventional security ideas into their sensor system [21][29]. So to shield the sensor system against from aggressor by obtaining the thoughts from current security plan is a decent answer for improved the sensor system security.

3.3 Sink hole Attack

Sinkhole attack is an insider attack was a gatecrasher trade off a node inside the system and dispatches an attack. At that point the tradeoff node attempt to pull in all the movement from neighbor nodes in view of the routing metric that utilized as a part of routing convention. When it figured out how to accomplish that, it will dispatch an attack. Because of correspondence example of wireless sensor system of numerous to one correspondence where every node send information to base station, makes this WSN powerless against sinkhole attack [22].

3.4 Wormhole Attack

In a commonplace wormhole attack, the assailant gets bundles at one point in the system, advances them through a wireless or wired connection with a great deal less inertness than the default joins utilized by the system, and after that transfers them to another area in the system. In this it is accepted that a wormhole is bi-directional with two endpoints, in spite of the fact that multi-end wormholes are conceivable in principle. A wormhole gets a message at its "inception end" and transmits it at its "destination end." Note that the assignment of wormhole closures as beginning and destination are reliant on the setting [23][26]. In addition a wormhole is detached (i.e., it doesn't communicate something specific without getting an inbound message) and static (i.e., it doesn't move).

3.5 Hello Flood

Some routing conventions in WSN oblige nodes to telecast hi messages to declare themselves to their neighbors. A node which gets such a message might accept that it is inside of a radio scope of the sender.

However now and again this suspicion might be false; now and again a tablet class assailant TV routing or other data with sufficiently substantial transmission power could persuade each other node in the system that the aggressor is its neighbor. For instance, an enemy publicizing a top notch course to the base station could make an extensive number of nodes in the system endeavor to utilize this course. However, those nodes which are adequately far from the foe would be sending the bundles into blankness. Henceforth the system is left in a mess. Conventions which rely on upon limited data trade between neighboring nodes for topology upkeep or stream control are fundamentally influenced by this sort of attack. An aggressor does not as a matter of course need to build honest to goodness activity to utilize the welcome surge attack [24][27]. It can essentially re-telecast overhead bundles with enough energy to be gotten by each other node in the system.

4. DEFENSE SCHEMES AGAINST ATTACKS

In this section, we present different schemes that can be used to counter attacks in wireless sensor networks. These classifications reflect many design choices for such security algorithms. Basically hundreds of algorithms have been proposed and we present only the algorithms which are suitable for this survey work.

To conquer the transport layer flooding Denial of Service (DoS) attack Aura, Nikander and Leiwo recommend utilizing the customer riddles postured by Juels and Brainard [11] in an effort to observe a node's dedication to making the association by using some of their own assets. Atmosphere et al. advocate that a server ought to compel a customer to confer its own particular assets first. Further, they recommend that a server ought to dependably constrain a customer to confer more assets in advance than the server. This system would likely be effective as long as the customer has computational assets tantamount to those of the server.

A proposed strategy to protect against the Sybil attack is to utilize irregular key pre-appropriation strategies [7]. In arbitrary key pre-conveyance, an irregular arrangement of keys or key-related data are doled out to every sensor nodes, so that in the key set-up stage, every node can find or process the basic keys it offers with its neighbors. The basic keys are utilized as shared mystery session keys to guarantee node to-node mystery. Newsome et al. recommend that the personality of every node is connected with the keys doled out to the node [7]. With a constrained set of caught keys, there is a little likelihood that a self-assertively created personality will work.

B.Yu [6] proposes a technique to identify sink hole attacks taking into account checkpoints. Firstly picking a few nodes along the way arbitrarily as the checkpoints node, then in the wake of getting information bundles, there will produce comparing affirmations and after that transmit them to the upper way. In the event that any checkpoints node doesn't get enough affirmations, it will produce cautioning messages to the source node, so that the location of the particular sending attacks can be figured it out. However, a clear issue exists in this procedure is that the nodes need to send affirmations consistently, which will enormously build the expense of the system. By the way, this strategy can't pass judgment on whether there pernicious alter activity exists.

Khalil, Bagchi and Shroff [4] proposed a lightweight countermeasure (LITEWORP) for wormhole attack identification utilizing protect nodes. In the wake of recognizing wormhole, LITEWORP takes off system in that open mode just, bringing about probability of more disturbance. To defeat this, they proposed another convention MOBIWORP [12], which expels malevolent nodes from the system utilizing focal power either locally or universally. Chen, Lou, Sun and Wang [16] introduced a protected restriction approach that can recognize simplex also, duplex wormhole attacks. They extended this calculation [14] to make it successful for different transmission scope of sensor nodes additionally, yet at the same time numerous wormholes can't be distinguished by this.

Multi-path multi-base station data forwarding technique is proposed in [19], in which a sensor node maintains number of different secrets (keys) in a multiple tree. Sensor node can forward its sensed data to multiple routes by using these secrets. There are multiple base stations in the network that have control over specific number of nodes and also, there are common means of communication among base stations. Each base station has all the secrets that are shared by all the sensor nodes, covered by it, according to the key assignment protocol [28]. Given the shared secret and the generated new key between two sensor nodes, the process of route setup requires much processing hence is inefficient.

Table 1 Summary

5. SUMMARY OF ATTACKS

A comprehensive study of the presented attacks is summarized in table 1, including the attack type, its characteristics, a possible solution and the damage it may cause. The table shows the detailed and required parameters and methods to fix the future research problems in this area. The table summarizes only the important attacks and their respective counter attacks in this vast research area. Conventional systems and objectives suited to the one of kind requirements of wireless sensor systems. The security objectives are named essential and auxiliary [5]. The essential objectives are referred to as standard security

objectives, for exampleClassification, Integrity, Authentication and Availability (CIAA).

	Attack	Characteristics	Counter Attack	Effect of the Attack
1	Denial of Service	Pernicious nodes advances most messages and specifically drops, which implies tossing away a portion of the information	Multipath Routing	The result will be a total hanging up of all the services offered by the network
2	Sybil	Vindictive node assumes various singularities. The point is to fill the memory of the neighboring node with futile information	Validation technique	Complete degradation of the network's service, depending on the site of the commencement of the attack.
3	Sinkhole	Malignant node acts as a dark gap and tries to draw all likely movement through a traded off node making an allegorical sinkhole with the enemy at the inside	quintessential scheme	Create a blackhole/sphere of influence in the sensor network
4	Worm hole	Vindictive nodes listen stealthily the parcel and can burrow messages gotten in one part of the system over a low inertness interface and retransmit them in a diverse part. It can be used to abuse routing race conditions	simple four way handshaking messages exchange	Routing race conditions characteristically occur when a node takes some action based on the first instance of a message it receives and afterwards ignores later messages.
5	Hello flood	It utilizes HELLO parcels as a warhead to convince the WSNs sensors. Conventions contingent upon the restricted data swaps between contiguous nodes for topology maintaining or stream control are moreover range under discourse. It can likewise be thought of as restricted, show wormholes.	identity verification protocol	If the attacker subsequently advertises minimum-cost routes, nodes will attempt to forward their messages to the attacker

6. RESEARCH DIRECTIONS

Taking after exploration issues for security in WSNs are especially vital:

i. Private Key operations on sensor nodes:

Previous studies on open key cryptography have demonstrated that open key operations might be handy in sensor nodes. On the other hand, private key operations are still extremely costly to acknowledge in sensor nodes. As open key cryptography can extraordinarily facilitate the outline of security in WSNs, enhancing the effectiveness of private key operations on sensor nodes is very appealing.

ii. Secure routing schemes for sensor systems:

Sensor nodes have incredible impact on sensor system topology and in this manner on the routing conventions. Mobility can be at the base station, sensor nodes, or both. Current conventions accept the sensor system is stationary. New secure routing conventions for versatile sensor systems need to be produced.

iii. Scalability and productivity:

Novel plans with higher adaptability and effectiveness should be produced for confirmed show of protocols. The late

advance out in the open key cryptography might encourage the outline of verified show conventions.

iv. Defending attacks:

Protecting attack is an awesome test. In the easiest from of this attack, a foe endeavors to disturb correspondence by transmitting a show sign of high quality. The enemy can likewise repress correspondence transmitting so as to abuse the MAC convention outlines while a neighbor is additionally by transmitting or by persistently asking for channel access with a solicitation to-send (RTS). New procedures for managing these attacks are required.

v. QoS and security:

Node execution is by and large corrupted with the expansion of security administrations in WSNs. Current studies on security in WSNs concentrate on individual themes such as key administration, secure routing, secure information accumulation, and interruption recognition. Security administrations should be assessed to high standards to achieve enhanced QoS.

7. CONCLUSIONS

On account of WSN, security has been an undeniably huge subject. Because of asset constraints, it is entirely difficult to give a solid security to a WSN. In the present paper, attacks and resistances referenced from 1997 till 2015 have been compressed and specific arrangements were proposed. Despite the fact that researches endeavors have been made on cryptography, key administration, secure routing, secure information collection, and interruption discovery in WSNs, there are still a few difficulties to be tended to. To begin with, the choice of the proper cryptographic strategies relies on upon the handling ability of sensor nodes, demonstrating that there is no brought together answer for all sensor systems. Rather, the security instruments are very application-particular. Second, sensors are described by the requirements on vitality, calculation ability, memory, and correspondence transfer speed. The configuration of security administrations in WSNs must fulfill these limitations. Third, the greater part of the present conventions accept that the sensor nodes and the base station are stationary. Be that as it may, there might be circumstances, for example, front line situations, where the base station and potentially the sensors should be versatile. The versatility of sensor nodes impacts sensor system topology and accordingly brings numerous issues up in secure routing conventions.

REFERENCES

[1] A Zhijun Li and Guang Gong “Survey on Security in Wireless Sensor Networks”, IEEE Computer Communications, Vol 8, No 2 ,PP 2-10. 2006.

[2] L. Hu and D. Evans. Secure aggregation for wireless networks. In SAINT- W ’03: proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT’03 Workshops), page 384. IEEE Computer Society, 2003.

[3] Jaydip Sen, “A Survey on Wireless Sensor Network Security”, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, August 2009, PP 55-78.

[4] I .Khalil, S .Bagchia n d N . B. S h r o f f , ”LITEWORP: ALightweightCountermeasure for theWormholeAttackinMultihopWirelessNetwork”,inInternationalConference onDependableSystemsandNetworks(DSN), pp.1-22,2005.

[5] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. In Revised Papers from the 8th International Workshop on Security protocols, pages 170–177. Springer Veri Log.

[6] B Yu, B Xiao. “Detecting selective forwarding attacks in wireless sensor networks”. In: Proe. of the 20th International Parallel and Distributed Processing Symposium, RhodesIsland, Greeee, 2006,1218-1230 nger-Verlag, 2001.

[7] R Nichols and P Lekkas. Wireless security: models, threats, and solutions. 2002.

[8] D. Braginsky and D. Estrin. Rumor routing algorthim for sensor networks. In WSNA ’02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 22–31, New York, NY, USA, 2002. ACM Press.

[9] A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT.

[10]Khalil,SaurabhBagchiandNessB.Shroff,“MOBIWORP:MitigationoftheWormholeAttack” inMobileMultihopWireless Networking and Ad-HocNetworks,vol. 6, no. 3,pp.344-362,2008

[11]HonglongChen,WeiLou,XiceSunandandZhiWang,“ASecureLocalizationApproachagainst WormholeAttacksUsingDistanceConsistency”,in HindawiPublishingCorporation EURASIPJournalonWireless CommunicationsandNetworking,vol.2010,11pages,2010

[12] Honglong Chen,WeiLou,XiceSunandZhiWang, “SLAW: SecureLocalizationAgainst Wormhole AttacksUsingConflicting Sets”, in Technical Report, The Hong KongPolytechnicUniversity,pp.1- 11,2010.

[13] N a i t F a r i d Nait-Abdesselam, BrahimBensaouandTarikTaleb, “Detecting andAvoiding WormholeAttacksinWirelessAd HocNetworks”,inproceedingof Wireless Communications and NetworkingConference,pp.3117-3122,2007.

[14]GuptaandS.Khurana,“SEEEP:Simpleandefficientend-to-end protocoltosecureadhoc networks against wormhole attacks” , in the Fourth International conference on Wireless Mobile Communication. 2009.

[15] N .GuptaandS.Khurana,“FEEPVR:FirstEnd-to-Endprotocol toSecureAdhocNetworks with variable range sagainst Wormhole Attacks”,in Second International Conferenceon Emerging Security

Information,SystemsandTechnologies –SECURWARE '08,pp.74-79,2008
[16] JakobEriksson, SrikanthV. Krishnamurthy and MichalisFaloutsos,," TrueLink: A Practical Countermeasure tot h e WormholeAttackinWireless Networks",in 14thIEEEInternational Conference on NetworkProtocols,pp.75-84,2006.
[17] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices", In Proceedings of the International Workshop on Security Protocols (IWSP), Lecture Notes in Computer Science(LNCS), 1997.
[18] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks", In Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications", pp. 22-31, New York, NY, USA, 2002, ACM Press.
[19] T. Aura, P. Nikander, and J. Leiwo, "DOS-resistant authentication with client puzzles", In Revised papers from the 8 th International Workshop on Security Protocols, pp. 170-177, Springer-Verlag, 2001.
[20] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M.B. Srivastava, "On communication security in wireless ad-hoc sensor networks", In Proceedings of 11th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002, pp. 139-144.
[21] P. Albers and O. Camp, "Security in ad hoc networks: A general intrusion detection architecture enhancing trust-based approaches", In Proceedings of the 1st International Workshop on Wireless Information Systems, 4th International Conference on Enterprise Information Systems, 2002.
[22] H. Chan and A. Perrig, "Security and privacy in sensor networks", IEEE Computer Magazine, pp. 103-105, 2003.
[23] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J. Tang, "Framework for security and privacy in automotive telematics", In Proceedings of the 2nd ACM International Workshop on Mobile Commerce, 2000.
[24] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", In Proceedings of the 2nd ACM Workshop on Security on Ad Hoc and Sensor Networks, Washington DC, USA, 2004.
[25] W. Du , J. Deng, Y.S. Han, and P.K. Varshney, "A pair-wise key pre-distribution scheme for wireless sensor networks", In Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 42-51, New York, NY, USA, 2003, ACM Press.
[26] R. Anderson and M. Kuhn, "Tamper resistance- a cautionary note", In Proceedings of the 2nd USENIX Workshop on Electronic Commerce, Oakland, California, 1996.
[27] A.R. Beresford and F. Stajano, "Location privacy in pervasive computing", IEEE Pervasive Computing, Vol. 2 No. 1, PP 46-55, 2003.
[28] Deepika Thakral and Neha Dureja " A Review on Security Issues in Wireless Sensor Networks", International journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 7, July 2012. PP 269-273.
[29] Danilo de Oliveira Gonçalves and Daniel G. Costa, "A Survey of Image Security in Wireless Sensor Networks", International journal of Imaging, Vol 4 No 3 2015, PP 5-30.

Authors Profile

Ram Pradheep Manohar, an M.E in Embedded System Technology graduate from Arulmigu Kalasalingam College of Engineering, Srivilliputhoor, Anna University and Electronics and Communication Engineering from Sun College of Engineering and Technology,Nagercoil, Manonmanium Sundarnar University, Tirunelveli, India. His research interest is in the area of wireless communication, Network Security, Sensor Networks, Communication networks.

E. Baburaj received his bachelor degree in Computer Engineering from Madurai Kamaraj University, India in the year 1992. He did his master degree in Computer Science and Engineering from the same University in the year 2002. He completed his PhD in Computer Science and Engineering from Anna University, Chennai in the year 2009. Dr. Baburaj is currently working as Professor of Computer Science and Engineering Department, Sun College of Engineering, Nagercoil. He has published more than 50 research papers in reputed international conferences and journals. His main research interest is Computer Networks and Cloud Computing that includes but not limited to Mobile Ad-hoc and Sensor Networks, Information-Centric Networking and Network Security.