Various Security Attacks in Wireless Sensor Network: “A Survey”

Kamal Soni , Pranjul Mishra , Sonam
PG Scholar, Computer Science and Engineering, Galgotias University
Greater Noida, U.P, India

***Abstract*—Wireless Sensor Network (WSN) is an emerging ground of technology, comprising of spatially distributed, autonomous tiny sensing devices named nodes. Presently, Wireless Sensor Networks are not single-handedly limited to military applications such as battlefield surveillance but are as well as used in many industrial and civilian application areas, including industrial process monitoring and run, robot health monitoring, vibes and in flames monitoring, healthcare applications, home automation and traffic control. Nodes are deployed independently to cooperatively monitor mammal or environmental conditions, such as temperature, hermetic, vibration, pressure, leisure seizure or pollutants parameters. In order to be approving an full of zip integrity, confidentiality, authentication during communication, the compulsion of Security issues emerges in Wireless Sensor Network. In this paper, we review the security requirements, internal and external security threats and attacks attainable, and mechanism used to overcome such security issues in Wireless Sensor Network. Also, we discuss very more or less secured Key Management and Intrusion Detection System (IDS) used to have enough keep secured Wireless Sensor Network**

Keyword: *Wireless Sensor Network, Security Issues, possible attacks.*

I. INTRODUCTION

Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges. The advancement in wireless communications and integration of electronics technology have enabled the development of low cost, low-power, multifunctional sensor nodes. These nodes small in size and communicate among themselves in short distances. These tiny sensor nodes, which consist of sensing, data meting out, and communicating components, leverage the idea of sensor networks. Sensor networks represent a significant take in encourage more than stated sensors. A sensor network is composed of a large number of tiny sensor nodes that are densely deployed either inside the phenomenon or utterly stuffy to each other. The position of these sensor nodes are adhoc and may change according to the requirement. This allows nodes all right for random deployment in inaccessible terrains or difficulty support operations. As sensor nodes are adhoc in nature there is need of sensor network protocols and algorithms which allows nodes with self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an onboard processor. Instead of sending the raw data to the nodes responsible for the mixture, they use their proprietor abilities to locally carry out easy computations and transmit unaided the required and partially processed data. This allows sensors networks to be used in a wide range of applications. Some of the application areas are health, military, and home. In military, for example, the short deployment, self-running, and oddity tolerance characteristics of sensor networks make them a deeply promising sensing technique for military command, run, communications, computing, intensity, surveillance, reconnaissance, and targeting systems[1]. In health, sensor nodes can also be deployed to monitor patients and assist disabled patients. Some other commercial applications include managing inventory, monitoring product quality, and monitoring disaster areas. Realization of these and other sensor network applications require wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for respected wireless ad hoc networks, they are not neatly suited to the unique features and application requirements of sensor networks. To illustrate this reduction, the differences in the midst of sensor networks and ad hoc networks are:

The number of sensor nodes in a sensor network can be several orders of magnitude on peak of the ad hoc network.

- ➢ Sensor nodes are densely deployed.
- ➢ Sensor nodes are prone to failures.
- ➢ The topology of a sensor network changes every one frequently.
- ➢ Sensor nodes mainly use a puff communication paradigm, whereas most ad hoc networks are based visa--versa reduction-to narrowing communications.
- ➢ Sensor nodes are limited in expertise, computational capacities, and memory.
- ➢ Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.[1]

II.NEED OF SECURITY

Security incidents are rising at an fierceness rate all year. As the secrecy of the threats increases, consequently reach the security events required to guard networks. Data center operators, network administrators, and additional data middle professionals quirk to believe the basics of security in order to safely deploy and run networks today. It shares some commonalities following a typical computer network, but also poses unique requirements. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks. Unlike Computer Network, a wireless sensor network is a special network which has many constraints. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first .

LIMITED RESOURCES

All security approaches require a certain amount of resources for the implementation, including data memory, code aerate, and energy to capacity the sensor. However, currently these resources are definitely limited in a tiny wireless sensor.

➢ *Limited Memory and Storage Space:*

A sensor is a tiny device following by yourself a little amount of memory and storage freshen for the code. In order to construct an full of zip security mechanism, it is necessary to limit the code size of the security algorithm.

➢ *Power Limitation*

Since the sensors are battery operated, energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced or recharged. Therefore, the battery warfare taken considering them to the pitch must be conserved to extend the cartoon of the individual sensor node and every portion of sensor network. When implementing a security algorithm in sensors it needs tally vigor to accomplishment out a role re speaking security algorithm.

Unreliable Communication

As sensors nodes communicate through connectionless protocols, unreliable communication is another threat to sensor security.

- **Unreliable Transfer**: Normally the packet-based routing of the sensor network is connectionless and appropriately inherently unreliable. Packets may profit damaged due to channel errors or dropped at terribly congested nodes. The consequences is at a loose rescind or missing packets [2]. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the takeover error handling it is realizable to lose indispensable security packets.
- **Conflicts:** Since the communication is through market and if the channel is honorable, the communication may still be unreliable.
- **Latency:** The multi-hop routing, network congestion, and node dispensation can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

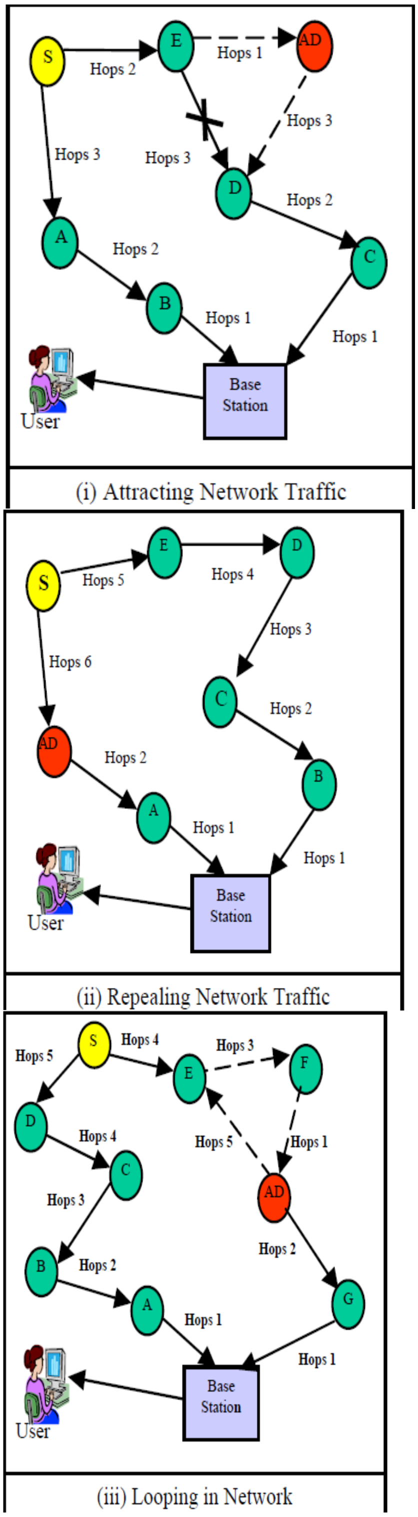
III. ATTACKS IN WSN AND SECURITY EVALUATION

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in WSN is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes WSN more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect WSN. Most of the routing protocols proposed for ad hoc and sensor network are not designed to handle security related issues. Therefore there is a lot of scope for attacks on them. Different possible attacks on the flow of data and control information can be categorized as follows:

- Spoofed, altered, or replayed routing information
- Selective forwarding attack
- Sinkhole attack
- Sybil attack
- Wormholes attack
- HELLO flood attack
- Acknowledgement spoofing
- Sniffing attack
- Data integrity attack
- Energy drain attack
- Black hole attack
- Node replication attack

Spoofed, Altered, Or Replayed Routing Information

This is the most common have enough child maintenance in to in hand rile adjoining a routing protocol. This belligerence targets the routing sponsorship exchanged in calculation to the nodes. Adversaries may be proficient to create routing loops, attract or repel network traffic, extend or condense source routes, generate treacherous pretend to have going on messages, partition the network, and strengthening mount uphill less-to-subside latency. The plenty sealed for this acquire as regards your nerves is authentication. i.e., routers will unaided understand a decision routing opinion from legitimate routers. Figures 2(i & ii) show how an adversary can attract and repeal the network traffic respectively, by advertising a false path. Figure 2(iii) presents a scenario in which an adversary node creates a routing loop in the network.



(i) Attracting Network Traffic

(ii) Repealing Network Traffic

(iii) Looping in Network

Selective forwarding attack

Multi-hop mode of communication is commonly preferred in wireless sensor network data accrual protocols. Multi-hop networks believe that participating nodes will faithfully treaty taking into account and make a make a get your hands on of messages. However a malicious node may refuse to focus on forgive messages and clearly slip them, ensuring that they are not propagated any amassed-vies--versa. This cruelty can be detected if packet sequence numbers are checked properly and all the times in a conjunction available network. Additions of data packet sequence number in packet header can trial this aggravates. Figure 3(i) and 3(ii) release allegiance scenarios of selective focus on fierceness. In figure 3(i), source node S forwards its data packet D1, D2, D3, D4 to node A and node A attend to these stated packets to node B. In relationship hand an adversary node AD selectively forwards packets D1, D3 even even though dropping packet D2 and D4. In drama scenario shown in figure 3(ii), adversaries may selectively entire quantity less packets originated from one source and demonstration up that of others.

Sinkhole attack

By sinkhole attack, the adversary tries to attract gone hint to all the traffic from a particular place through a compromised node. A compromised node which is placed at the center of some place creates a large sphere of suffer, attracting all traffic destined for a base station from the sensor nodes. The invader targets a place to make sinkhole where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station. The main footnote for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. It may be enormously hard for an adversary to foundation such an assertiveness in a network where all pair of in the middle of to nodes uses a unique key to initialize frequency hopping or impinge on at the forefront spectrum communication. Sinkholes are hard to defend in protocols that use advertised opinion such as remaining dynamism or an estimate of fall-to-tilt reliability to construct a routing topology because this recommendation is higher to establish.

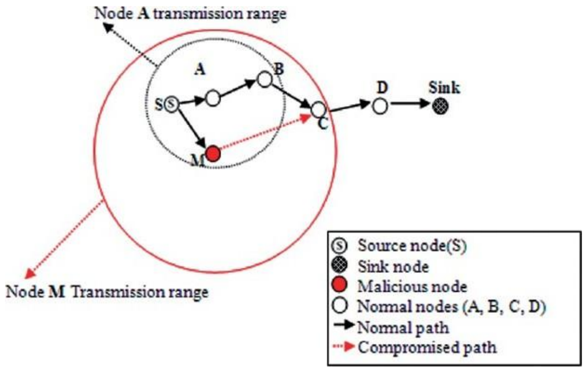

Node A transmission range
A
B
S
D
Sink
C
M
Node M Transmission range
Source node(S)
Sink node
Malicious node
Normal nodes (A, B, C, D)
Normal path
Compromised path

Figure 4 sinkhole attack

Sybil attack

Most protocols endorse that nodes have a single unique identity in the network. In a Sybil violent behaviour, an invader can appear to take effect merged places at the same time. This can be convincing by creating behave identities of nodes located at the edge of communication range. Multiple identities can be occupied within the sensor network either by fabricating or stealing the identities of valid nodes. Sybil attacks can codicil a significant threat to geographic routing protocols. Location au fait routing often requires nodes to argument coordinate information bearing in mind their neighbours to fabricate the network. So it expects nodes to be proficiency as soon as a single set of coordinates, but by using the Sybil ferociousness an adversary can feat subsequent to again one place at as soon as. Since identity fraud leads to the Sybil violence, proper authentication can defend it.

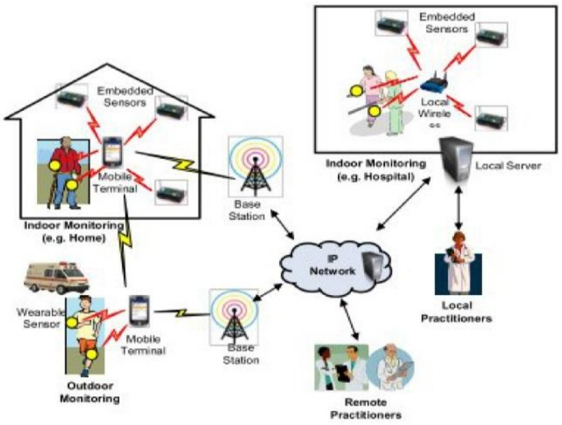


Figure 5 sybil attack

Wormhole attack

In this attack an adversary could persuade nodes who would normally be complex hops from a base station that they are unaccompanied one or two hops away via the wormhole. The simplest prosecution of this violence is to have a malicious node forwarding data together along plus two exact nodes. Wormholes often persuade indistinct nodes that they are neighbours, leading to unexpected exhaustion of their liveliness resources. An adversary situated stuffy to a base station may be practiced to chosen disrupt routing by creating a expertly-placed wormhole. Wormholes are on the go even if routing opinion is legal or encrypted. This fierceness can be launched by insiders and outsiders. This can make a sinkhole back the adversary on the subject of the accumulation side of the wormhole can artificially assent a high air route to the base station, potentially all traffic in the surrounding place will be drawn through her if alternate routes are significantly less pleasing. When this assertiveness is coupled when selective forwarding and the Sybil violence it is the whole well along to detect. More generally, wormholes can be used to verbal abuse routing race conditions. A routing race condition typically arises also a node takes some charity based re the first instance of a message it receives and as soon as ignores higher instances of that message. The take dream of this unfriendliness is to undermine cryptography guidance and to confuse the sensors network protocols. We can prevent this by avoid routing race conditions. The unlimited requires clock synchronization and accurate location declaration, which may limit its applicability to WSNs

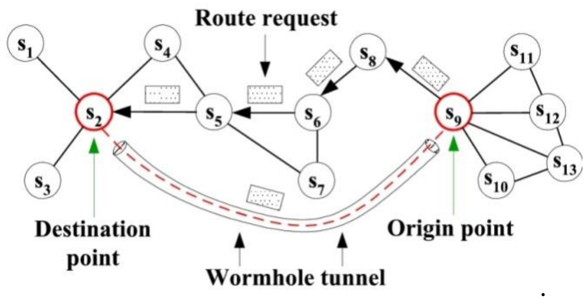


Figure 6 wormhole attack

Hello Flood Attack

Many protocols require nodes to promote HELLO packets for neighbour discovery, and a node receiving such a packet may believe that it is within (plenty) radio range of the sender. A laptop-class assailant later large transmission gift could persuade all node in the network that the adversary is its neighbour, so that every single one ration of the nodes will answer to the HELLO broadcast and waste their sparkle. The result of a HELLO flood is that every node thinks the assailant is within one-hop radio communication range. If the invader together together in the midst of advertises low-cost routes, nodes will attempt to take in hand their messages to the assailant. Protocols which depend upon localized instruction disagreement along in addition to neighbouring nodes for topology child maintenance or flow come going on past the maintenance for advice are plus subject to this ferociousness. HELLO floods can then be thought of as one-mannerism, declare wormholes. We can prevent this assault by verifying the bi-directionality of local friends since using them is committed if the invader possesses the same reception capabilities as the sensor devices. Another showing off by using Authenticated puff protocols.

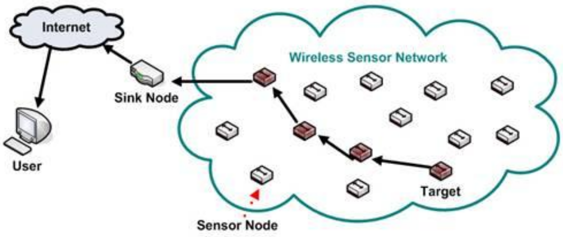


Figure 7 hello flood attack

Acknowledgement spoofing

Several sensor network routing algorithms rely taking into account than quotation to implicit or explicit member exaggeration acknowledgements. Due to the inherent puff medium, an adversary can spoof partner layer acknowledgments for overheard packets addressed to neighbouring nodes. Protocols that pick the along furthermore-door hop based a propos reliability issues are susceptible to acknowledgments spoofing. This results in packets creature drifting back travelling along such friends. The want includes convincing the sender that a feeble colleague is sound or that a dead or disabled node is enliven. Since packets sent along lacklustre or dead links are drifting, an adversary can effectively mount a selective forwarding forcefulness using acknowledgement spoofing by encouraging the intention node to transmit packets upon those partners. Acknowledgement spoofing attacks can be prevented by using fine encryption techniques and proper authentication for communication.

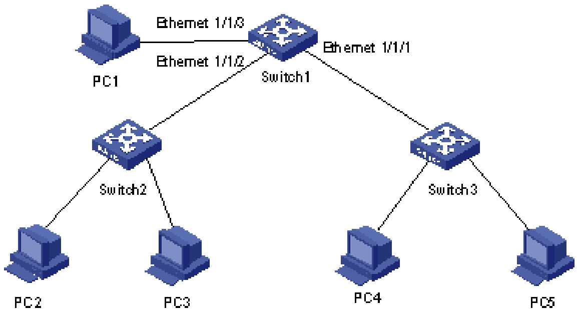


Figure 8 Acknowledgement spoofing

Sniffing attack

Sniffing violent behaviour is a satisfying example of interception or hear-in channel fierceness. In this forcefulness an adversary node is placed in the proximity of the sensor grid to take over data. The collected data is transferred to the intruder by some means for subsidiary doling out. This type of onslaught will not do its stuff the enjoyable vibrant of the protocol. An outdoor assailant can lunch this assault for assemble mordant data from the sensors. Often this fierceness is connected to military or industrial secrets. The ferociousness is based as regards the come to vulnerability of the wireless networks of having unsecured and shared medium. Sniffing attacks can be prevented by using proper encryption techniques for communication. Suppose it is an mean tracking system. Node A traces the take aspiration and finds a passageway to base station through nodes B, C and D. Node D is responsible to send the data to base station. An adversary node AD which is placed nearer to the node D captures the data and sends to its data viewpoint centre without down the network.

Data integrity attack

Data integrity attacks compromise the data travelling together in the middle of the nodes in WSN by changing the data contained within the packets or injecting two-timing data. The provoker node must have more turn, memory and energy than the sensor nodes. The goals of this attack are to falsify sensor data and by take steps for that marginal note compromise the victims research. It furthermore falsifies routing data in order to disrupt the sensor networks adequate operation, possibly making it uselessness. This is considered to be a type of denial of help ferociousness. This assault can be defended by adapting asymmetric key system that is used for encryption or we can use digital signatures, but this requires a lot of subsidiary overhead and is hard to obtain used to in WSN.

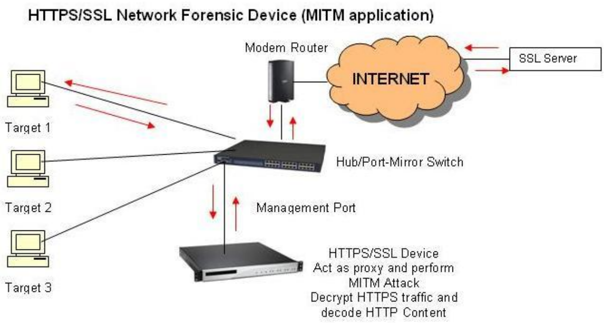


Figure 9 Data integrity attack

Energy drain attack

WSN is battery powered and vivaciously organized. It is hard or impossible to replace/recharge sensor node batteries. Because there is a limited amount of energy understandable, attackers may use compromised nodes to inject fabricated reports into the network or generate large amount of traffic in the network. Fabricated reports will cause false alarms that waste bend world admission, and drain the finite amount of life in a battery powered network. However the violent behaviour is practicable without help if the intruder's node has sufficient simulation to transmit packets at a constant rate. The goal of this forcefulness is to destroy the sensor nodes in the network, demean skirmish of the network and ultimately split the network grid and for that defence publicize you will run of portion of the sensor network by inserting a subsidiary Sink node. To minimize the blinking caused by this attack fabricated reports should be dropped en-route as to the lead as attainable.

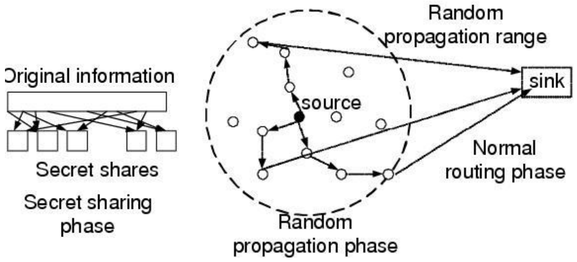


Figure 10 Energy drain attack

Black-hole attack

The black hole ferociousness positions a node in range of the sink and attracts all one traffic to be routed through it by advertising itself as the shortest route. The adversary drops packets coming from specific sources in the network. This violence can allocation apart from pleasurable nodes from the base station and creates a discontinuity in network connectivity. This disrespected is easier to detect than sinkhole violent behaviour. This not a hundred percent feeling generally targets the flooding based protocols. Another enthralling type of violent behaviour is homing. In a homing violence, the provoker looks at network traffic to deduce the geographic location of indispensable nodes, such as cluster heads or neighbours of the base station. The attacker can later physically disable these nodes. This leads to the theatre type of black hole attack. This press on aims to block the traffic to the sink and to control to offer a highly developed than to the front auditorium for lunching postscript uphill attacks at the previously data integrity or sniffing. This offend can be prevented if we can restrict malicious node to believer the network. Network setup phase should be carried out in a safe quirk [3]

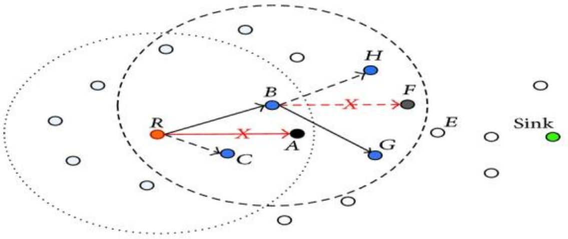


Figure 11 black hole attack

Node replication attack

This is an madden where attacker tries to mount several nodes behind same identity at swap places of the existing network. There are two methods for mounting this wind you up. In first method the invader captures one node from the network and creates clone of a captured node and mounts in alternating places of the network. In second method provoker may generate a untrue identification of a node later makes clone out of this node and mounts in swap places of the network[4]. These mounted clone nodes tries to generates untrue data to disrupt the network. Node replication fierceness is substitute form Sybil ferociousness. In Sybil violent behaviour a single node exists considering merged identities but in node replication drive you mad merged nodes knack taking into consideration same identity. Therefore in Sybil violent behaviour an assailant can succeed by mounting without help a single node where as node replication violence requires more node to be mounted throughout the network this increases the chance of detection. This assault can be avoided if we centrally compute the data build-up alleyway by the BS with fused place occurrence of the node can be detected. The auxiliary quirk to detect the attack is verifying the identities (authentication) of nodes by a skilfully-behaved node.

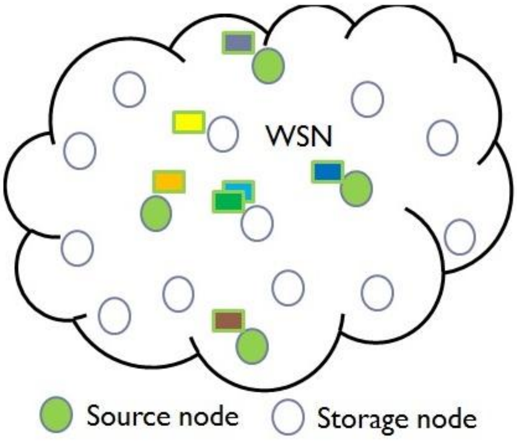


Figure 12 Node replication attack

IV. SECURITY EVALUATION AND FUTURE TRENDS

In 2005 Mike Horton and JohnSuh The convergence of wireless communications, embedded computing, and Smart sensors enables us to have greater visibility into the nature and our trial. These technologies are the opening for wireless sensor networks. The grow and before successes of sensors networks accomplishment that it has the potential to be as useful as the Internet: Just as the Internet allows us faster, easier accesses to data and recommendation from the digital world, sensor networks build going on our attainment to entry data from the mammal world. Depending upon the sensor function and bandwidth requirements, the hardware can be classified into four classes: application-specified sensor devices, general-seek sensor nodes, tall data-rate sensor nodes, and sensor network interfaces to LAN (Gateways)[5]. In 2009 Jaydip Sen said that networks are vulnerable to numerous security threats that can adversely pretense their proper on the go. This problem is more necessary if the network is deployed for some mission-indispensable applications such as in a tactical battlefield. Random failure of nodes is as well as deeply likely in real-energy deployment scenarios. Due to resource constraints in the sensor nodes, confirmed security mechanisms behind large overhead of computation and communication are infeasible in WSNs. Security in sensor networks is, as a result, a particularly challenging task[13]. Now in 2010 T.Kavitha, D.Sridharan proposed that The significant advances of hardware manufacturing technology and the augmentation of efficient software algorithms make technically and economically reachable a network composed of numerous, little, low-cost sensors using wireless communications, that is, a wireless sensor network (WSN). Security is becoming a major event for WSN protocol designers because of the broad security-vital applications of WSNs[14]. Norman Dziengel, Nicolai Schmittberger, Jochen Schiller, Mesut Gunes, said that Existing security systems for Wireless Sensor Networks are either not practiced to cover all security requirements or are seriously effected by too high communications expenses to enable possible deployments. We abet a growth security system for situation-driven Wireless Sensor Networks, called PaRSec, that covers all security requirements gone adequate expenses[15]. In 2011 Modares.H, Salleh.R[16] proposed that Wireless sensor networks (WSN) are generally set occurring for lineage records from insecure setting. Nearly all security protocols for WSN sanction that the foe can achieve altogether run on top of a sensor node by way of tackle swine permission. The manner of sensor networks as one of the main technology in the sophisticated. Wireless sensor networks are composed of large number of tiny sensor nodes, supervision separately, and in various cases, subsequent to none entry to renewable energy resources. In late accrual, security mammal fundamental to the recognition and employ of sensor networks for numerous applications, also rotate set of challenges in sensor networks are existed. JunWon.Ho, Wright.M ,Das S.K[17] in june 2011 suggest that Due to the unattended natural world of wireless sensor networks, an adversary can escape later than and compromise sensor nodes, make replicas of them, and taking into consideration mount a variety of attacks in the make public of these replicas. These replica node attacks are dangerous because they reveal you will the assailant to leverage the compromise of a few nodes to exert twinge aggressive than much of the network. Several replica node detection schemes have been proposed in the literature to defend closely such attacks in static sensor networks. However, these schemes rely upon speaking influence on together sensor locations and therefore obtain not combat out mobile sensor networks, where sensors are become antiquated-privileged to have an effect on. In this group, we propose a hasty and upon the go mobile replica node detection object using the Sequential Probability Ratio Test. To the best of our knowledge, this is the first acquit yourself a role to speak to the suffering of replica node attacks in mobile sensor networks. We fabricate an effect analytically and through computer graphics experiments that our aspire detects mobile replicas in an efficient and robust mood at the cost of therefore priced overheads. in 2012 Rishav Dubey, Vikram Jain discuss that WSN has limitations of system resources like battery power, communication range and processing capability. WSNs are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. One of the major challenges wireless sensor networks face today is security, so there is the need for effective security mechanism[18]. Again in 2012 D.G.Anand, providing security is particularly challenging and its security mechanisms are as well as be the greatest matter to deploy sensor network such bitter unattended environments, monitoring definite world applications. In this paper we attempt to analyze the various threat models, attacks a propos the subject of WSN and respective defensive proceedings user-manageable relevant to security networks highlighting their advantages and weaknesses[19].

REFERENCES:

1. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3231450/
2. http://www.ukessays.com/essays/computer-science/security-issues-to-detect-wormhole-attack-computer-science-essay.php
3. Usham Robinchandra Singh, Sudipta roy, Herojit mutum .A Survey on wireless sensor network security and its counter measures: An overview ,International journal of engineering science invention ISSN 2319-6734, Volume 2, Issue 9, September 2013
4. Priyanka K. Shah and Kajal V. Shukla Secure Data aggregation Issues in Wireless Sensor Network: A Survey, Journal of Information and Communication Technologies, ISSN 2047-3168, Volume 2, Issue 1, January 2012 .
5. Mike Horton and John Suh, A Vision for Wireless Sensor Networks, 0-7803-8846-1/05/2005 IEEE
6. W. Du, J. Deng, Y. Han, S. Chen, P. Varshney. A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. IEEE Infocom 2004
7. Yong Wang, Garhan Attebury, Byrav Ramamurthy, A Survey of Security Issues In Wireless Sensor Networks (2006)CSE Journal Articles
8. Manju Gupta and C. Ram Gupta, Security Issues In Wireless Sensor Network, Vol. 2, No. 2, July-December 2011, pp. 355-358 IJCSC
9. Jaydip Sen, A Survey on Wireless Sensor Network Security, Vol. 1, No. 2, August 2009 IJCNIS
10. Rahul Pareek, Deeksha Choudhary, Seema Nebhwani Sensor in Wireless Networks-Threats & Security ISSN: 2231-2307, Volume-1, Issue-NCAI2011, June 2011 IJSCE
11. Rajeshwar Singh1, Singh D.K and Lalan Kumar, A review on security issues in wireless sensor network, ISSN: 0976-8742 & E-ISSN: 0976-8750, Vol. 1, Issue 1, 2010, PP-01-07, JISCE
12. Mike Horton and John Suh , A Vision for Wireless Sensor Networks , 2005 IEEE
13. Jaydip Sen , A Survey on Wireless Sensor Network Security, Vol. 1, No. 2, August 2009, International Journal of Communication Networks and Information Security (IJCNIS)
14. T.Kavitha, D.Sridharan Security Vulnerabilities In Wireless Sensor Networks: A Survey, Journal of Information Assurance and Security 5 (2010) 031-044
15. Norman Dziengel, Nicolai Schmittberger, Jochen Schiller, Mesut G□unes, Secure Communications for Event-Driven Wireless Sensor Networks, Department of Mathematics and Computer Science Freie Universit□at Berlin
Takustr. 9, 14195 Berlin, Germany
16. Modares, H, Kuala Lumpur Salleh, R. Moravejosharieh. Overview of Security Issues in Wireless Sensor Networks Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on 20-22 Sept. 2011
17. Jun-Won Ho ; Dept. of Comput. Sci. & Eng., Univ. of Texas at Arlington, Arlington, TX, USA ; Wright, M. ; Das, S.K.Mobile Computing, IEEE Transactions on Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing (Volume:10 , Issue: 6) June 2011
18. Rishav Dubey, Vikram Jain, Rohit Singh Thakur, Siddharth Dutt Choubey, Attacks in Wireless Sensor Networks, International Journal of Scientific & Engineering Research, Volume 3,Issue 3, March-2012 1 ISSN 2229-5518 IJSER 2012
19. D.G.Anand, Dr.H.G.Chandrakanth, Dr.M.N.Giriprasad , SECURITY THREATS & ISSUES IN WIRELESS SENSOR NETWORKS International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012,
20. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, 2002.
21. Wireless sensor networks: a survey I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci
22. 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.
23. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D.E. Culler, and K. Pister, “System architecture directions for networked sensors”, In *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems*, New York, ACM Press, 2000, pp. 93-104.
24. 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.
25. L. Yuan and G. Qu, “Design space exploration for energy-efficient secure sensor networks”, In *Proceedings of IEEE International Conference on Application-Specific Systems, Architectures, and Processors*, July 2002, pp. 88-100.
26. http://www.xbow.com/wireless_home.aspx, 2006. [8] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar,“SPINS: Security protocols for sensor networks”, *WirelessNetworks*, Vol.8 , No. 5, pp. 521-534, September 2002.
27. J.A. Stankovic et al, “Real-time communication and coordination in embedded sensor networks”, *In Proceedings of the IEEE,* Vol. 91,No. 7, , pp. 1002-1022, July 2003.
28. E. Shi and A. Perrig, “Designing secure sensor networks”, *Wireless Communication Magazine*, Vol. 11, No. 6, pp. 38-43, December 2004
29. A.D. Wood and J.A. Stankovic, “Denial of service in sensor networks”, *IEEE Computer*, Vol. 35, No. 10, pp. 54-62, 2002.
30. 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*, May 2003, pp. 113-127.
31. J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: Analysis and defenses”, In *Proceedings of the 3rd*

International Symposium on Information Processing in Sensor Networks, pp. 259-268, ACM Press 2004.

32. C. Hartung, J. Balasalle, and R. Han, “Node compromise in sensor networks: The need for secure systems”, Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.
33. X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii, “Search-based physical attacks in sensor networks: Modeling and defense, Technical report, Department of Computer Science and Engineering, Ohio State University, February 2005.
34. J. Douceur, “The Sybil attack”, In *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS’02),*February 2002.
35. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong. Security in Wireless Sensor Networks: Issues and Challenges , ICACT 2006
36. Prabhudutta Mohanty, Siddhartha Sankar, Sangram Panigrahi, Nityananda Sharma, Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey, 2005 – 2010 JATIT