A Survey on Attacks and Issue in Wireless Sensor Networks

S. Vanathi
Assistant Professor
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research, Chennai, T.N- 600 073, India

Abstract— Wireless Sensor Network (WSN) is an infrastructure-less wireless link that is arranged in a huge number of wireless sensors in an ad-hoc routine that is used to display the system, carnal or ecological conditions. The sensor nodes have extreme source limitations, unreliable communication medium and that too in unattended environments. This makes it very difficult for the implementation of the existing security approaches to WSNs due to the complexity of the standing algorithms. Aspect study of these attacks will help in the design of robust and efficient countermeasures for attacks in contradiction of WSNs.

Keywords: Wireless Sensor Network, Sensor, Security, Security Mechanism

I. INTRODUCTION

Wireless Sensor Networks (WSN) are developing as both an imperative new tier in the IT network and a rich province of active investigate involving hardware and system design, networking, distributed procedures, programming models, data management, security and social factors. The basic idea of sensor network is to dissolve tiny sensing devices; which are proficient of sensing some changes of parameters and collaborating with other devices, over a specific terrestrial area for some precise purposes like target chasing, observation, environmental monitoring. Today's sensors can monitor infection, burden, humidity, soil makeup, vehicular measure, rattle levels, lighting conditions, the occurrence or nonappearance of certain kinds of constituents, automatic stress levels on attached objects,and other possessions. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The attractive structures of the wireless sensor networks attracted many researchers to work on various issues related to these types of grids. However, while the routing approaches and wireless sensor network modeling are getting much preference, the refuge issues are yet to obtain all-embracing focus.

II. ATTACKS IN WIRELESS SENSOR NETWORKS

Attacks in contradiction of wireless sensor networks might be approximately careful from two unrelated levels of views. One is the existence against the safety diplomacies and another is against the undeveloped devices. Here we theme out the foremost occurrences in wireless device networks.

A. Denial of Service

Denial of Service is shaped by the inadvertent disappointment of nodes or malicious action. The simplest DoS attack attempts to devour the possessions accessible to the mark node, by distribution extra unnecessary packets and thus prevents authentic network users from retrieving services or belongings to which they are eligible. DoS attack is predestined not only for the challenger's shot to destabilize, dislocate, or extinguish network, but also for any event that reduces a network's capability to offer a service. In wireless sensor networks, numerous types of DoS attacks in different layers might be performed.

At physical deposit the DoS occurrences could be tailback and intrusive, at link layer, rear-ender, exhaustion, iniquitousness, at network layer, desertion and greed, homing, misdirection, black holes and at transport layer this attack could be performed by hateful overflowing and desynchronization. The mechanisms to prevent DoS attacks include recompense for network resources, pushback, strong confirmation and documentation of traffic.

B. Node Outage Attack

The node outage attack is suspending the functionality of WSN mechanisms and the attacks apply actually or sensibly in network. The belongings of this attack are discontinuing the lump services such as reading, gathering and launching the functions. The attack is fitting to amendment model and obtainability and legitimacies are main intimidations for this occurrence in web.

1) Tampering: It is the effect of physical access to the bulge by an assailant; the determination will be to recover cryptographic significant like the keys used for ciphering.
2) Black hole: A node fabricates routing evidence to force the way of the data by itself, later on; its only assignment is then nothing to transfer creating a sink or black hole in the system.
3) Selective forwarding: As mentioned above a node play the part of router in a selective hastening attack malevolent node may garbage to advancing certain communications and simply drop them.
4) Sybil attack: Definite this attack by: "malicious device, taking numerous identities in an illegitimate way", attacker can use the personalities of the others nodes in order to take part in disseminated algorithms such as the election.
5) HELLO flood attack: Many direction-finding protocols use "HELLO" packet to determine adjacent nodes and thus to found a topology of the link. The simplest occurrence for an aggressor consists in conveyance a flood of such communications to flood the network and to avoid other messages from being replaced.
6) Jamming: A well-known attack on wireless communiqué, it consists in disturbing the radio channel by sending useless information on the occurrence band used. This jamming can be momentary, intermittent.
7) Blackmail attack: A malevolent node makes proclaim that another sincere node is spiteful to eliminate this last from the network. If the malicious node accomplishes to confrontation a momentous number of protuberances, it will be able to disturb the process of the network.

8) Exhaustion: Its used to consume all the properties energy of the target node, by obliging it to do calculations or to receive or diffuses upper fluously data.
9) Wormhole attack: Attackers here are intentionally placed at different ends of a network. They can receive communications and reiterations them in dissimilar parts by resources of a channel.
10) Identity replication attack: Attacker can clone nodes and place it in dissimilar part of the link in directive to accumulate mainstream of evidence traffic. Disparate the Sybil attack, the uniqueness repetition attack is based upon giving the same individuality to different physical nods. This attack can be straddling because in a WSN there is no way to know that a wireless sensor node is compromised.

III. Solutions over attacks

The issue of link layer encryption can be addressed with the support of discerning accelerating and sinkhole The Sybil occurrences can be stopped. The wormhole concept can make use of sequestered channelized approach. HELLO flood is alternative foremost contest which can be addressed by authenticating the bi-directionality of a link the issue of an interloper substantiation can be determined using a globally collective key.

This also confirms discriminating accelerating and stops sinkhole and Sybil occurrences. For well-organized selective accelerating multi-path routing and routing based on probabilistic approach can be used Sinkhole can be made more efficient, robust and better by authentication of routing metric data for instance the latent energy, available energy.

IV. Security schemes

Zigbee refuge scheme is keying over hardware-based proportion featured Multipath and multiphase routing based stations and confirmation in bi-directional aspects is another security scheme which accepts secret sharing in probabilistic method to overwhelmed the Hello Flood Attacks The security of announcement can be addressed with effective and coherent data deceiving standby organization which certifies defense of the network as a whole. TIK security scheme faces wormhole attacks, tricking of the available information and data.

This is done with the assistance of symmetric cryptography requiring accurate time synchronization amongst all parties comprised in the communiqué aspect. The en-route filtering based on statistics faces information spoofing to be one of the major threats. The detection and dropping false reports during advancing process is ensured as an implicit feature TinyPK, TinySecprotection scheme faces Data and information spoofing, message replay as the major attacks. The underlying features comprising message authenticity, confidentiality while working in link layer of the architecture. SNEP and µTESLA face similar issues and problems as of TinyPK and TinySec providing replay protection, weak freshness and low message overhead as the highlighting features.

SMECN which characterizes Small Minimum Energy Statement Network along with LEACH shortened as Low Energy Adaptive Clustering Hierarchy pose protocols for network layer of WSNs to be one of the significant threats. The different type addressing routing information through WSN along with results of finding and directing the packet along the most efficient and optimized path to traverse to its terminus comprises some of the structures.

V. Limitations of WSNs

Each and every type of security device needs specific amount of resources for its own device to function. The sensor nodes usually hold information, sequencer and energy which face their own borders Energy constraint issue: The factors leading to energy depletion need careful intervention which comprises of diverse characteristics such as total energy consumed in ingesting of security in encryption, decryption along the whole measure of energy spent in storage and refuge parameters for occurrence the ones concerning cryptography. Reminiscence restriction issue: It is alternative issue around which the crux of explanations turns to maintain an competent security mechanism with augmented recollection.

A. Changeability of message

One of the primary threats to device security is the very nature of the wireless message medium, which is integrally insecure. The wireless intermediate is open and accessible to anyone unlike wired networks, where a apparatus has to be actually connected to the medium. Due to this any diffusion can easily be intercepted, altered, or replay by an adversary. Intruder can easily intercept valid packets and inject malevolent ones due to open access nature of wireless communication medium.

Additionally, destructive of packets may take place due to unreliable broadcast channels, this may be result of channel errors or high congestion in sensor nodes. Even communication may still be untrustworthy in the case of unfailing channels also. Conflicts may occur due to packets colliding meet in the middle of transfer consequential in failure of transfer. Such weakness can be easily oppressed by an intruder having a strong transmitter, and can easily produce intervention.

B. Character and Massive Scale

A elevated quantity of dynamics in WSNs is caused due to join mobility, node failures, and ecological obstructions. Frequent topology changes and network partitions are the reasons for this. Sensor node can be deployed in large areas which is one of the most attractive characteristics of WSNs capability. Thousands or millions of nodes, without any prior knowledge on their position can be deployed making the configuration of the network complicated. It is therefore requisite that well-organized security schemes can activate within this dynamic background.

It is a extensive task of networking tens to hundreds or thousands of nodes and implementing security over such a network is equally tough too. More strong security techniques are required to cope with such dynamics of ever-changing nature of antenna networks. At the identical point in time change in the set of associations membership needs to be supported in an equally efficient and locked manner. There should be transparency regarding

node device fusion/exit the network and a least amount of in sequence ought to have to be reconfigured.

VI. CONCLUSION

The demand for protection in WSNs becomes more obvious during ability enlargement of WSNs and they are used a large amount more. Security in Wireless Sensor set-up is vital to the receiving and utilize of sensor networks. In meticulous, Wireless Sensor Network product in industry will not get acceptance unless there is a full proof security to the network. In WSNs the node nature causes boundaries like restricted energy, capacity of processing and storage capacity. These restrictions create WSNs so destructive from conventional Ad hoc wireless networks The security of WSNs has become a major focus since of the different dangers appearing and the significance of data in confidence, although in the past, there was a little absorption on WSNs security. This paper summarizes the attacks and their classifications in wireless sensor networks and also an endeavor has been made to discover the safety measures mechanism widely used to grip those attacks.

REFERENCES

[1] Douceur, J. "The Sybil Attack", 1st International Workshop onPeer-to-Peer Systems (2002).
[2] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensornetworks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004,pp. 259 – 268.
[3] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSRMANETs", Proc. First International Conference on Broad band Networks,2004, pp. 681 – 688.
[4] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September2003, pp. 293-315.
[5] Avancha, S, "A Holistic Approach to Secure Sensor Networks", PhD Dissertition, University of Maryland, 2005.
[6] Wood, A.D., Stankovic, J.A., and Son, S.H., "JAM: A Jammed-AreaMapping Service for Sensor Networks",24th IEEE Real-Time Systems Symposium, RTSS 2003, pp. 286-297.
[7] Cagalj, M., Capkun, S., and Hubaux, J-P., "Wormhole-basedAnti-Jamming Techniques in Sensor Networks" fromhttp://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf
[8] Hamid, M. A., Rashid, M-O., and Hong, C. S., "Routing Security inSensor Network: Hello Flood Attack and Defense", to appear in IEEEICNEWS 2006, 2-4 January, Dhaka.
[9] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security forSensor Networks", CADIP Research Symposium, 2002, available at,http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf
[10] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS:Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no.5, 2002, pp. 521-534.
[11] SunilGhildiyal, Ashish Gupta, MusheerVaqur, and Anupam Semwal, "Analysis of wireless sensor networks: security, attacksand challenges," International Journal of Research in Engineering and Technology, Volume: 03 Issue: 03, Mar-2014, eISSN:2319-1163, pISSN: 2321-7308

