Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 3(E), pp. 24966-24969, March, 2018

ISSN: 0976-3031

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

SYBIL ATTACK IN WIRELESS SENSOR NETWORKS

***Sunil Ghildiyal[1]., Himanshu Goel[2] and Surender Kumar Jangra[3]**

[1]Shri Venkateshwara University, Gajraula, UP
[2]Uttaranchal university Dehradun Uttarakhand
[3]GTB College, Bhawanigarh, Punjab

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0903.1762

ARTICLE INFO

Article History:

Received 05th December, 2017
Received in revised form 21st January, 2018
Accepted 06th February, 2018
Published online 28th March, 2018

Key Words:

Wireless, Node, Constraint, Sybil, Threat

ABSTRACT

Researchers have implemented many security architectures against security vulnerabilities in WSNs. but failed to provide any effective solutions, securing small, tiny and sophisticated nodes till the time. The main obstacles for applying any traditional security solutions are constraints within the architecture of WSN's. However, developments in last few years, implementation of less power micro-controllers based wireless sensors have been raised very fast as solution of real-world problems. A variety of attacks have been observed to attack these low powered, unattended nodes. Since nodes have limited power battery with a limited life, nodes are not able to perform traditional available security mechanisms or algorithms for prevention. Sybil attack is one of the harmful threat to wireless sensor networks, comprising a malicious node illegally forging an unbounded number of identities. Sybil attack is inspired by polymorphic behavior; having multiple identities simultaneously by a node. In such case, malicious node claims multiple identities or have fake Ids. It is typical but important to detect such guilty nodes from the infrastructure.. This paper aims to the introduction of wireless sensor network architecture, attacks, and attack detection methods. The significance of Sybil attack is also described in detail.

Copyright © Sunil Ghildiyal *et al*, 2018, this is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

For last about 20 years, Wireless Sensor Networks (WSNs) application and utility have attracted worldwide researchers. Along with the research in area of Micro-Electro-Mechanical systems (MEMS) technology, researchers facilitated the application and deployment of sensors in many problem solutions (Musheer 2014).Wireless sensor networks (WSN) technology proved itself as result oriented promise for many applications for mass public as well as defense(Neelam Srivastava *et.al.* 2010). These nodes are low RF based, limited duty cycle based, less power, low cost smart devices having processing constraints (Al. Sakib Khan *et. al.* 2006). But huge growth in demand of these nodes indicate how these can be utilized in variety of areas of real-life problem solving applications. Small sensor nodes are scattered or deployed over an area to sense the physical parameters like pressure, temperature or velocity as information, subsequently, processing the information(not all the nodes) , locally decision making, if needed and to forward the information to next available node in the network. These networks are applicable in distributed wireless sensing applications, cutting wired installation costs and critical situation simultaneously.

WSN Node Organisation

WSNs are applicable in many applications like military, traffic monitoring, patient monitoring and environment, also in real life applications like fire alerts and intrusion monitoring (Yong sik *et.al.* 2010). In WSN, multiple nodes are deployed over an area to detect or sense and record the physical parameters like pressure, velocity and humidity etc. and to redirect the recorded values to further network. A typical sensor node must have sensing, processing and communication capabilities for this purpose. These sensors may be deployed in order to get the crucial real-time data from the all the location, even where wired sensors cannot be deployed or human intervention is not possible due to critical situation (Warneke *et.al.* 2001). Nodes comprise of RF for sensing, less processing capabilities, low energy source. Sensor network itself restricts the nodes to perform complex processing or any traditional security measures due to its power limitations. Hence nodes are very sensitive to the vulnerabilities by many attacks and phenomenon (Watkins *et.al.* 2010) In WSN, a node supports multi-hop routing. The sensor based network is not infrastructure dependent, also does not need any pre-infrastructure or any access point as same is in any traditional

Corresponding author:* **Sunil Ghildiyal
Shri Venkateshwara University, Gajraula, UP

wired network. Sensors participate dynamically, situation based and in routing dynamically by forwarding the data they have sensed so far. To which node data is to be forwarded is also determined dynamically by the cluster head selection or election process. A sensor node must be operable on low power and to be operated in dense deployment environment as several nodes are densely scattered over an area to record the physical parameters and to forward them further. As the large number of nodes is required by an application, nodes must be cheaper and easily dispensable. One more feature about node's mechanism is that it must be environment adaptive and self organizing. As physical size is concerned, it is recommended to size of nodes is to keep small so preventing it from physical stealing and temper.

Generally, a node consists of a RF transceiver, low capable processing unit (micro-controller) and battery unit along with ADC/DAC and a sensor. Few node also comprise of external memory of few kb. Sensors node use RF for transmitting and receiving the communication with each other hence use broadcast basically. Wireless communication over the broadcast is difficult to protect cause of easy eavesdropping; injecting can be performed over broadcasting. Sensors nodes are deployed or scattered over an area totally insecure manner in terms of physical security, hence can be stolen, physically tempered easily. Any average attack can easily penetrate WSN security (Qinghua Zhang*et.al.* 2009). Limited resources make node weak and paralyzed in front of any intended flooding attack.

WSN Security Requirements

The use of security architecture is to prevent and protect the information from attackers. In wireless sensor networks security requirements make sure that network services are available even in presence of DoS and also in presence of any vulnerability. Only authorized WSN node can be involved in information passing. It also ensures that a malicious node cannot masquerade as trusted node easily. There has to be confidentiality and integrity in message, to make sure the authorization in network like what sent from authorized sender to receiver. Data freshness and non-repudiation is also to be taken into account with the security measures, applied or to be. Since the tiny sensor nodes are randomly deployed and operated in unattended environment like earthquake prone areas, so the security requirements include self-organization of node which further includes self-configuration, self-management (autonomous) and self-healing (fault tolerant).

WSN Attacks and Threat Models

In WSN, threats are from outside the network and within the network. If attacks are from the nodes of the native network then it is much harmful and not easily detected. Also, it is very tough to find out the malicious or compromising node within the native network. Another classification of the attacks may be passive and active where passive attacks don't modify or alter the information whereas active attacks do so. There is variety of attacks to the WSNs. For example if the opponent attack by using similar capacity nodes for network penetration it is called mote class attack but when much powerful devices like laptop are used to penetrate the security of the network then such attack is called laptop attack. Since the nodes are generally operated in unattended under uncontrolled conditions, there are number of attacks at its each layer. These attack may destroy the node physically, can damage route or routing tables, their formed topology, change the location and even at application layer like reprogramming etc. The attacks of WSN can be classified into two categories: invasive and non-invasive. Non-invasive attacks to the timings, power and frequency of channel, try to destroy signaling. Invasive attacks target to make services in DoS mode, transit path of information, routing directions etc. In DoS attack, hacker tries to make service or system inaccessible. However during the transit of information, more common attacks are encountered due to open air channel. Routing attacks are generally inside attacks. Most common routing attacks are False Routing or Spoofed, Altered, Replayed Routing Information, Selective Forwarding, Sinkhole Attacks, Sybil Attack, Wormhole, Hello Flood and. Acknowledgment Spoofing.

Sybil Attack

In Wireless sensor networks, mechanisms for redundancy are based on the identifications while entering in the network to participate. Each node is distinguished as its one unique entity and presents only an abstract concept of single identity. Hence, WSNs. and nodes are mush sensitive to any of the method which can forge the identity. One of such a malicious method is the *Sybil attack*. In Sybil attack, a node can be compromising one, may be intentionally or by force, presenting its identity illegal. Even this node may be changing the identities or having many false IDs. These multiple IDs. may be stolen IDs. also those of other nodes. A *Sybil node* is a misbehaving nodes extra identity than its native one. Therefore, a single entity may get selected many times (n number of identities) to participate in an network operation which is redundancy based, thereby taking control of outcome of the operation, and cheating the redundancy mechanisms (John R. Douceur *et.al.* 2006). Doueceur, was the first person who introduced the Sybil attacks on P2P architecture. Roosta also succeeded with their views on different way to detect and handle the Sybil attacks (J. Newsome *et.al.* 2004). Detailed analysis of Sybil attack was also proposed by Cemtepe and Yener in their own way (Jyoti Prakash singh *et.al.* 2008). Sybil attack are observed taking place in case of broadcast also where central administration for authorization is not present. Central administration helps in authorization and identification of identities of nodes. In Sybil attack, attacker can have multiple identities by sending messages with multiple identifiers. When a node illegitimately claims more than one identity or having multiple stolen identities, entire wireless sensor network suffers from Sybil attack. In actual, malicious node itself replicates its multiple identity copies in intention to damage the network. Sybil attack can be internal or external or both simultaneously. Authentication is a step to prevent from external Sybil attacks but not from internal. Most important is about Sybil attack is that attack is done by violating one-to-one mapping between identity and entity in WSN.

Sybil Attacks Types and Existing Methods

It is very important to know about the different forms of Sybil attack, which generally targets the network to get confused or damaged (M. Cardei *et. al.* 2005). Sybil attack Taxonomy is three dimensional taxonomy: 1. Direct vs. Indirect Communications 2.Fabricated vs. Stolen Identities

3.Simultaneity. In first type, legitimate nodes communicates directly with nodes however in case of indirect method, the communication in between legitimate node and other nodes is done through malicious nodes. Sybil attack may also take place due to fabricated and stolen identities. In case of fabricated identity, nodes can reprogram a similar fabricated ID for itself on the basis of structure of legitimate nodes ID. Nodes may also steal the legitimate nodes ID and can use it as their native ID. To measure such kind of attacks, stolen identities are to be destroyed. If the Sybil attack is simultaneous, all identities will participate in network at the same time. In non-simultaneous Sybil attack, attacker continuously presents a large number of identities over a period of time. Another kind of Sybil attack targets distributed storage, where Sybil attack on replication and fragmentation mechanism. In another case, Sybil attack on routing can also results multipath or disparity routing in, seemingly disjoint paths can go through a single malicious node presenting identities. Data aggregation Sybil attack are also applicable on specific sensor network protocols to manipulate the recording of sensors in order to conserve energy rather than returning individual original readings. Fair Resource Allocation Sybil attack can take place during fair resource allocation which will allow a promising node to obtain unfair share of resources. In misbehavior detection nodes can be used to spread the blame in a misbehavior detection network.

One of the existing methods to detect Sybil attack is based on the RF capability of each node of the network which already have got assigned a single radio channel capacity randomly to broadcast and listen. Lets assume that in network any physical device has only one radio and radio is incapable of simultaneously sending or receiving on more than one channel. Now every node is assigned a different channel to broadcast and different channel to listen. If the neighbor with assigned channel is legitimate then: let s is the total number of nodes and n is number of nodes then:

Prob. of detection = s/n
Prob. of non-detection = (n-s)/n
For r rounds: Prob. of non-detection = $((n-s)/n)^r$
In case there are no enough channels for assignment to the nodes then this method can face problem.

Registration is observed as one of the solution to prevent from Sybil attack. There may be one trusted central head or cluster head to acquire the node's identity. This central recording of identities can help in identifying the legitimate node as it to be checked in known-good list. But registration list which contains known identities, can also be targeted by attackers. If this list is compromised or hacked, then attacker's identity will also be treated as known-good.

Position verification is also applicable in case of rigid WSN nodes. If the nodes are immobile and will not be changing their position, this is one of the effective method for detecting Sybil attack. If any such attack is created by a malicious node, corresponding GPS position of the node will be changed and will be detected as Sybil attack as network had already recorded nodes initial physical or GPS positions.

Demerits of Existing Methods

Every of above method has its own tradeoffs. They are based on some predetermined assumptions and different costs , and can measure different type of attacks if attack is also based on those assumption tradeoffs. Many of them are power consuming and may require large processing which is not suitable with limited power and processing capability nodes. Like position verification can only put a bound on the number of nodes. Node registration requires human intervention in order to add node securely in the network which is not applicable in critical situations.

Proposed Solution

A typical WSN can be configured as combination of several nodes and one base station(BS). Nodes have limited processing power and limited battery life however BS is much powerful device like a workstation or laptop with much powerful power backup than ordinary nodes. Every node has its own identity $ID_{i.}$ It is assumed that nodes have embedded encryption key K_i, would be used for encryption by the node. Base station is central location which records the complete database of ids of every sensor node and corresponding encryption key (Zorbas. D. *et.al.* 2009). The solution is based upon a tree based hierarchical structure where BS is top and cluster heads (CH) nodes are at next level. These CH nodes are followed by other participating nodes at the last level. The circulation of information is configured as routed from sensor nodes to base station through CH necessarily. One BS may have interface with another BS of any other intra-network or any outside network any special network structure. These nodes organize themselves in self organized manner, subsequently into clusters, based on self-organizing clustering and cluster head deciding scheme and decide their CH, which is for communication from node to BS. LEACH has been observed as an efficient algorithm for deciding the cluster head. LEACH has a principle of rotation of assignment of cluster head to any node randomly but mainly on basis of remaining power. To extend power life, CH is responsible for node to be observed for active or sleep period or corresponding instances. Base station is assumed to have enough battery and memory space to communicate in a secure manner, while all other nodes in its jurisdiction and also with the any wired net. A sensor node i is assigned encryption key (K_i) along with a unique number $ID_{i\ .}$ This ID helps it to be recognized in the network. But assignment of keys to the sensor nodes via wireless medium is also not preferred due to security. Hence IDs. are assigned during the manufacturing process, whiel nodes are manufactured in the plants. Before deployment base station assigns all the ID numbers and K_is to be used in the network and records complete list of same. Now a malicious node with ID_m and K_m can be caught easily while entering for attack as its ID and Key does not match with the cluster head or base stations database. Even entry of any new node with valid ID is also not possible because of inbuilt keys which are burned in the chips. However base station generates session key for information exchange and broadcasts to all the cluster heads in the network. This session is relayed to the ordinary nodes by their respective cluster heads and also updated periodically with new session keys. Now information can be transferred only in between the trusted nodes by the use of appropriate encryption and decryption keys of respective nodes. All the information will be routed under the control of base station for their IDs. uniqueness along with keys. As BS holds all the records, malicious node cannot enter in the network. Since each and every node is having a pre-distributed key, the identities of the nodes are bounded. The malicious user cannot use fabricated identity outside the set of identities. But still stolen identity, man in the middle situation may harm our proposal and attack can somehow take place. Replay attack can also be prevented if a sequence number is used for communication.

CONCLUSION

WSN nodes have limited processing and less power life. It make them much susceptible for number of attacks. Nodes have limited resources and they have to be protected by some support from outside them like any powerful device within the network like BS. BS can only execute complex security processing and algorithms for security of entire network. Proposed solution against Sybil attack is based on pre-distributed keys of sensor nodes, embedded the time of manufacturing stage. Intentionally, Keys are pre-distributed and not distributed via any channel or communication. Solution resists Sybil attacks but, base station processing and its I/O traffic is going to increase heavily which is certainly a problem, is to be addressed in future solutions.

References

Musheer vaquar" Target Management Protocol for Wireless Sensor Network", IJAECSSE Jan 2014

Neelam Srivastava *"Challenges of Next-Generation Wireless Sensor Networks and its impact on Society"* Journal of Telecommunications, Volume 1, ISSUE 1, FEB 2010 128

Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong *"Security in Wireless sensor Networks: Issues and Challenges"* ISBN 89-5519-129-4 Feb 22-22, 2006 ICACT2006

Yong-Sik Choi, Jeon, Sang-Hyun Park *"A Study on Sensor Nodes Attestation Protocols in WSN"* ICACT 2010.

Warneke, B., Last, M., Liebowitz, B., Pister, K., Smartdust "Communicating with a cubic-millimeter computer" Computer 34, 1(2001), 44-51

G.M. Ben Ezovski, S.E. Watkins "The Electronic Sensor Node and the future of Government Issued RFID based identifications" RFID 2007, IEEE International Conference, pp 15-22, 2007

Qinghua Zhang, Pan Wang, Douglas S. Reeves, Peng Ning "Defending against Sybil Attacks in Sensor Networks" Cyber Defense Laboratory, Computer Science Department North Carolina State University, Raleigh, NC 27695-8207 2009

John R. Douceur, The attack, (2002), 251-260.

Tanya Roosta, S. P. Shieh, and Shankar Sastry, Taxonomy of security attacks in sensor networks and countermeasures, The First IEEE International Conference on System Integration and Reliability Improvements, December 2006.

J. Newsome, E. Shi, and D. Song, "The Attack in Sensor Network: Analysis & Defences," The Third Intl. Symposium on Information Processing in Sensor Networks (IPSN"04), Berkeley, California, USA: ACN Press, 2004, pp.185-191.

Jyoti Prakash singh *et. al*. "Defending Against Sybil Attacks in Sensor Networks using Pre-Distributed key" Durgapur Inst. of Adv. Tech. & Mgt. Durgapur WB. 2008

M. Cardei and D.-Z. Du, "Improving Wireless Sensor Network Lifetime through PowerAware Organization", ACM Wireless Networks, Vol. 11, No. 3, pp. 333-340, May 2005.

Zorbas, D., Glynos, D. & Douligeris, C, "Connected partial target coverage and network lifetime in wireless sensor networks", Wireless Days (WD), 2009 2nd IFIP, pp. 1-5

How to cite this article:

Sunil Ghildiyal *et al*.2018, Sybil Attack In Wireless Sensor Networks. *Int J Recent Sci Res.* 9(3), pp. 24966-24969.
DOI: http://dx.doi.org/10.24327/ijrsr.2018.0903.1762

****