International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Analysis of Sybil Attack in Wireless Sensor Networks

Sunil Ghildiyal[1], Ashish Gupta[2], Nitesh Tomar[3], Anupam Semwal[4]
[1]Uttaranchal University, Prem Nagar Dehradun
[2] Dev Bhoomi Inst. of Technology, Dehradun
[3] Dev Bhoomi Inst. of Technology, Dehradun
[4]IEC University, Atal nagar, Baddi, Distt.: Solan

Abstract- **Many security mechanisms against security threats in WSNs. have been deployed for many years , but no any effective solutions regarding the implementation of same have been found out till time . The main constraints for applying any effective security solutions are constraints in WSN's own architecture However, developments in last many years, implementation of low power micro-controllers based wireless sensors have been rapidly increased in solving real-world problems. Many attacks may attack these low powered, unattended nodes. Since nodes have small battery with a limited life, nodes may not perform complex security algorithms for prevention from attacks. Sybil attack is dangerous threat to wireless sensor networks, consisting a malicious node illegally forging an unbounded number of identities to defeat redundancy mechanisms. Sybil attack is inspired by having multiple identities simultaneously by a node. In this attack a node, claims multiple identities or having fake Ids. It is important to detect such faulty nodes in large peer to peer architecture. This paper aims to the introduction of wireless sensor network architecture, threats and attack detection methods.**

Key Words: Wireless, Sensor, Power, Sybil ,Threat, Key

I. INTRODUCTION

In last two decades, Wireless Sensor Networks (WSNs) application and usefulness have attracted worldwide attention. Specially with the advancements in area of Micro-Electro-Mechanical systems (MEMS) technology which has facilitated the research and deployment of sensors[1].Wireless sensor networks (WSN) technology has provided result oriented promise for many applications for mass public as well as defense[2]. These nodes are low duty cycle based, low power, low cost smart devices having computational constraints[3]. Rapid grow in demand of these sensor nodes indicates how these can be utilized in many areas of real-life problem solving applications. Tiny sensor nodes are deployed over an area to sense the physical parameters like pressure, temperature, humidity as information, subsequently, processing the information, locally decision making, if needed and to communicate the information to next node in the network. These networks are implemented in distributed wireless sensing applications, cutting wired installation costs and limitations simultaneously. The recent research and advancements in area of micro-controllers and wireless technologies have resulted as cheap, low power communication wireless sensor nodes, which can be deployed densely over an area to record the physical parameters. Sensor nodes have a limited battery life before they exhaust last. However nodes may be equipped with alternatives to energy harvesting units like solar, vibrations or wind energy but still energy issue in WSN is to be addressed efficiently.

II. WSN AND NODE ARCHITECTURE

WSNs are applied to many fields of applications like military, traffic monitoring, patient monitoring and environment, also in real life applications like fire alerts and pollution monitoring [4]. In WSN, several nodes are deployed over an area to sense the physical parameters like pressure, velocity and humidity etc. and to forward those to further network. Hence 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 critical location, where wired sensors cannot be deployed or human intervention is not possible [5]. Nodes comprise of sensing hardware, less processing capabilities, low communication capabilities and low energy source. Sensor network itself restricts the nodes to perform better processing, security measures due to its power limitations. Hence nodes are vulnerable to many attacks and phenomenon [6].

In WSN, a node supports multi-hop routing. The sensor based network is not dependent on any pre-infrastructure or any access point as same is in any wired network. Sensors participate in routing dynamically by forwarding the data they have sensed so far. To which node data is to be forwarded is also determined dynamically. A sensor node must be operable on low power ad 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 dispensable. One of the important factors about node's mechanism is that it must be environment adaptive. For physical point of view, 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 communicating unit (RF transceiver), processing unit (micro-controller) and power unit along with ADC/DAC and a sensor. Node also comprises of external memory. Sensors node use RF for 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 scattered over an area physically insecure manner, hence can be stolen, physically tempered easily or after capturing such node physically, any logical

security mode can easily be detected or penetrated [7]. Limited resources of the node make it weak and paralyzed in front of any intended flooding attack. Initial measure against such threats is to utilize the sensors for their maximum capabilities to make network fully functional within authorized access and resources. Keeping size of nodes very small is also one the measure to make it safe from physical stealing and tempering.

III. SECURITY REQUIREMENTS IN WSN

The aim of security mechanism is to protect the information from attacks. In wireless sensor networks security requirements make sure that network services are available even in presence of DoS and also in presence on any vulnerability. Only authorized WSN node can be involved in information passing. It also ensures that a malicious node cannot masquerade as trusted node. There has to be confidentiality and integrity in message, 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 so the security requirements include self-organization of node which further includes self-configuration, self-management (autonomous) and self-healing (fault tolerant).

IV. THREAT MODEL & ATTACKS

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. Also, it is quite difficult 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 data as active attacks do. If the opponent attack by using similar capacity nodes for network penetration it is called mote class attack but when powerful devices like laptop are used to penetrate 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 harm the node physically, can damage routing, topology, 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 generally target to timings, power and frequency of channel. Invasive attacks target to availability of service, transit of information, routing etc. In DoS attack, hacker tries to make service or system inaccessible.

However during the transit of information, more common attacks are encountered. 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.

V. SYBIL ATTACK

In Wireless sensor networks, mechanisms for redundancy are identity-based. It is assumed that each node is distinguished as one entity and presents only one single abstract concept of an identity. Hence, WSNs. and nodes are vulnerable to any method which allows identities to be forged or falsified. Such a malicious method is the *Sybil attack*. In Sybil attack, a single node intentionally, illegally presents many false or forge identities to other nodes in the network by either new (false) identities, or stealing legal identities from others. A *Sybil node* is a misbehaving node's extra identity. Therefore, a single entity may get selected many times (depends on number of identities) to participate in an network operation that relies on redundancy, thereby controlling the outcome of the operation, and defeating the redundancy mechanisms[8].

Doueceur introduced the Sybil attacks on P2P architecture first time [9]. Roosta ET. Al. also presented their views on variety and defense mechanisms against Sybil attacks [10]. Detailed analysis of Sybil attack was also proposed by Cemtepe and Yener [11].

Sybil attack can take place while broadcasting without any central authority. This central authority may help in identifying the identities of nodes. Attacker can have different identities by sending messages with multiple identifiers. When a node illegitimately claims many identities or having multiple stolen identities, WSN suffers from Sybil attack. The such malicious sensor node itself replicates its multiple copies to damage the network. There can be Sybil attack internally or externally. Authentication may somehow prevent from external attacks but not from internal. One of important observation about Sybil attack is that it attacks on the violation of one-to-one mapping between identity and entity in WSN.

VI. ATTACKS TAXONOMY AND TYPES

It is very important to know about the different forms of Sybil attack, which have targeted the network to get confused or damaged [12].
Sybil attack Taxonomy is three dimensional taxonomy: 1. Direct vs. Indirect Communications 2.Fabricated vs. Stolen Identities 3.Simultaneity.

In direct method of Sybil attack, legitimate nodes communicates directly with nodes however in case of indirect method, communication in between legitimate node and nodes is done via malicious nodes. Sybil attack may also include fabricated and stolen identities. In case of fabricated identity, nodes creates similar fabricated ID for it on the basis of structure of legitimate node's ID. nodes may also steal the legitimate node's ID and can use it as its own ID. Such attacking nodes will not be identified till stolen ID is destroyed. If the Sybil attack is simultaneous, all identities will participate in network at same time. In non-simultaneous Sybil attack, attacker presents a large number of identities over a period of time.

Main types of Sybil attacks are Distributed Storage, Routing, Data Aggregation, Voting, Fair Resource Allocation and Misbehavior Detection. In case of Distributed Storage, there is Sybil attack on replication and fragmentation mechanism. 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 affect on some sensor network protocols to aggregate the reading of sensors in order to conserve energy rather than returning individual readings. Fair Resource Allocation Sybil attack can be used in fair resource allocation which will allow a malicious node to obtain unfair share of resources. In Misbehavior Detection nodes can be used to 'spread the blame' in a misbehavior detection network.

VII. EXISTING DETECTION METHODS

A. Radio Resource Testing

This method is based on the radio capability of each node of the network which already have got assigned a single radio randomly to broadcast and listen. Let's 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.

B. Registration

Registration may be one of the effective solution to prevent from Sybil attack. There may be one trusted central authority to know the node's identity. This can help in identifying the legitimate node as it to be checked in known-good list. But registration list which contains known identities, has to be protected from malicious nodes. If any attacker could add its identity in this list then identity will be treated as known-good.

C. Position Verification

In this method it is assumed that 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 position of the node will be changed and will be detected as Sybil attack as network had already recorded node's initial positions.

D. RSSI Based

In this method, localization algorithm is used. By having the position of nodes on signal strength, presence of attack in network can be calculated. Upon receiving a message, the four detector nodes compute the location of sender and associate this location with the sender-ID included in the message. But location calculation is costly.

VIII. DEMERITS OF ABOVE METHODS

Each of above method has its own tradeoffs. Every method is based on different assumptions and different costs , and can measure different type of attacks not all. Like radio resource method demand energy, 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.

IX. 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[13].

We assume a tree based hierarchical structure where BS is at the top and cluster heads (CH) are at next level. These CH are followed by ordinary nodes at the lowest level. Information is always routed from sensor nodes to base station through CH. BS interface with another BS of outside network any special structure during deployment. But these nodes their selves However, these nodes organize themselves into clusters, based on self-organizing clustering

decide their CH, which is for communication from node to BS. LEACH is an efficient algorithm for deciding the cluster head. LEACH has a principle of assignment of cluster head to any node randomly and on basis of remaining power. To extend battery 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 style, while all the nodes in its jurisdiction and also with the any wired extra-net.

Each 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 secure. Hence IDs. are assigned during the manufacturing process. Before deployment base station assigns all the ID numbers and K_i's 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 base station's database. Even entry of any new node with valid ID is also not possible because of inbuilt keys. However base station generates session key for information exchange and broadcasts to all CH in the network. This session is relayed to the ordinary nodes by their respective cluster heads and also updated time to time with new session keys.

Now information can be transferred only in between the trusted nodes by the use of 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

Limited processing capability and less power of WSN nodes 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. Keys are pre-distributed as it is not recommended to distribute the keys through unsecured wireless network links. 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

[1] Neelam Srivastava *"Challenges of Next-Generation Wireless Sensor Networks and its impact on Society"* JOURNAL OF TELECOMMUNICATIONS, VOLUME 1, ISSUE 1, FEB 2010 128

[2] 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

[3] Ritu sharma, Yogesh Chaba and Y.Singh "*Ánalysis of Security Protocols in Wireless Sensor Network"* International Journal Avanced Networking and Applications Volume 02, issue 03, pages:707-713(2010)

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

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

[6] 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

[7] Ritu sharma, Yogesh Chaba, Yudhvir Singh "Analysis of security protocols in wireless sensor networks" Int. Journal Advanced Networking and Applications Vol 02, Issue 03.

[8] 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

[9] John R. Douceur, The attack, (2002), 251–260.

[10] 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."

[11] Seyit A. Camtepe and B¨ulent Yener, Key distribution mechanisms for wireless sensor networks: a survey.

[12] 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.

[13] Jyoti Prakash singh et. Al. " Defending Against Sybil Attacks in Sensor Networks using Pre-Distributed key" Durgapur Inst. of Adv. Tech. & Mgt. Durgapur WB.