ISSN:0975-9646
Sandeep Sindhu et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 4102-4105

Techniques to Alleviate Sybil Attack and Security Issues in Wireless Sensor Network

Sandeep Sindhu
PG Scholar
Deenbandhu Ch. Choturam
University of science & technology
Murthal ,Sonipat

Dr.Suman Sangwan
Astt.Professor
Deenbandu Ch.Choturam
University of science & technology
Murthal ,Sonipat

Abstract-It is quite a difficult task to achieve security in a wireless sensor network because sensors have limited battery backup, dynamically changing topology, lack of central management and infrastructure. A particular harmful attack that takes the advantage of these characteristics is the Sybil attack.Sybil attack, in which a single malicious node illegitimately claims multiple identities. This attack can extremely disrupt various operations of the wireless sensor networks such as voting, data aggregation, data replication and data fragmentation, fair resource allocation scheme, misbehavior detection and routing mechanisms.

Keywords: Wireless sensor network, Sybil attack.

1. INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes .Wireless Network can be classified into two types one is Infrastructure based and other is Ad-hoc network. In Infrastructure based network each user needs to communicate with an access points or base stations whereas in Ad-hoc wireless network consists of (usually mobile and wireless) nodes that create and maintain their intercommunication links without the help of a pre-existing infrastructure. There is not any central controller is present. Security in Ad hoc networks are difficult because links between nodes are unreliable as well as their network topology is dynamic. Sensor nodes perform various tasks such as signal processing, computation, and network self-configuration to expand network coverage and strengthen its scalability. A WSN is composed of tens to thousands of Sensor Nodes which are distributed in a wide area. These sensors are small and able to sense, communicate and process data with each other, in general over a radio frequency channel. Sensors have tiny, low battery-powered, self contained, small cost devices. A sensor is a device that measures pressure, light, temperature, and transform it into a signal which can be read by a human or by an instrument. The basic task of sensor networks is to sense the node, gather data and send it to their requested destination. In case of traditional wired networks have enough storage capacity, unlimited power, fixed network topologies, wide communication range and computational capabilities. These features make the traditional networks able to meet the communication demands. On the other hand, WSNs are resource constrained distributed systems with low energy, low bandwidth and short communication range.

2. ISSUES IN WIRELESS SENSOR NETWORK

Controlling a large range of application types in WSN is not an easy with single Concept and design of the wireless network

2.1 Hardware and operating system for WSN

In our environment sensor node are deployed sensor node are used to find out the change to physical environment like humidity, sound and pressure. Sensor network are small and significant energy limitation.

2.2 Wireless radio communication

Wireless sensor network performance depends on the quality of wireless communication. In sensor network wireless communication is unpredictable in nature.

2.3 Medium access schemes

Energy consumption is higher in wireless communication and radio of the nodes is the network is directly control by MAC protocol influences the life time of the network by regulating the energy consumption.

2.4 Deployment

Deployment of sensor nodes can be done either by placing nodes one after another in sensor field or by dropping it from a plane. Deployment means locating and operational sensor node in a real world environment .Deployment of sensor node in network is a diligent activity as we do not have effect over the quality of wireless communication.

2.5 Localization

Sensor localization is a main and important issue for network management and operation. In many of the real world scenario no infrastructure and advance deployment position is available to locate and management of deployment. To finding the physical location of the sensors node after they have been deployed is known as the problem of localization.

2.6 Synchronization

Clock synchronization is a main service in sensor network. In a sensor network time synchronization goal to provide a common time scale for local clock of nodes in the network. In a sensor system a global clock will help process and analyze the data correctly and predict future system behaviour. Global clock synchronization is use in some application like environment monitoring, vehicle tracking, navigation guidance etc.

2.7 Calibration

Calibration is the process of maintaining the raw sensor reading taken from the sensor into corrected values by comparing it with some standard values. In a sensor

network manual calibration of sensor is a time consumes and difficult task due to failure of sensor nodes and random noise which make manual calibration of sensor too expensive.

2.8 Data aggregation

Data gathering involves systematically collection the sensed data from multiple sensor and transmitting the data to the base station for further process. Data generated from sensor is often redundant and data transfer to base station is huge. Data aggregation is defined as the process of aggregation the data from multiple sensors to elimination redundant transmission and estimation the desired answer about the sensed environment, then provide fused information to the base station.

2.9 Quality of service

Quality of service is the level provided to the users present in sensor network. Quality of service for sensor network is the minimum number of sensor sending information toward base station. Since sensor network are used in mission critical application such as military application and nuclear plant monitoring applications. Quality of service in these situation are of utmost importance.

3 SYBIL ATTACK

When a single illegitimately node claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself into network to make many copies to destroy and collapse the network. The system can attack internally or externally. The attack which occur from outside from network can be prevented by authentication but internal attacks are not prevent by this. There should be one to one mapping between identity and entity in WSN. But due to this attack one-to-one mapping is violated by creating multiple identities.

3.1 Dimensions of Sybil Attack

Sybil attack can be represented using three dimensions: Communication,Participation and Identity.

3.1.1 Direct and Indirect Communication:

In direct communication, all legitimate nodes in network communicate directly with Sybil nodes. A legitimate node sends a message to a Sybil node, one of the malicious devices listens to the messagewhereas in indirect communication, the communication is done through malicious node.

3.1.2 Fabricated and stolen identities:

A new identity is created by comparing based on the identities of the legitimate nodes, that is, if legitimate nodes have an ID with length 16 bit integer, it randomly creates ID of 16 bit integer. This node is called fabricated identities.

In stolen identities, attacker stolen the legitimate identities and then uses it. In this way the attacker is not identified in the network if the node whose identity has been stolen is destroyed. Identity replication is done when the same identities are used many times in the same places.

3.1.3 Simultaneous and non-simultaneous attack:

When all the Sybil node participate in the network at the same time than this is known as simultaneous attack . The number of identities the attacker uses is equal to the number of physical devices; each device presents different identities at different times.

In non-simultaneous, Sybil nodes participate the network one by one when one Sybil node leave the network another node become active.

4 TYPES OF SYBIL ATTACK

4.1Routing

Sybil attacks can destroy routing protocols of networks, mainly the multicast routing mechanism. In multipath routing protocol, if the Sybil attacker has presented multiple Sybil nodes among the legitimate nodes, then for the legitimate sender nodes it may appear that the route request packets are being forwarded through different paths, whereas they are being actually passed through a single malicious node

4.2 Distributed Storage

Douceur [2] observe that replication and fragmentation mechanism in peer to peer storage system is defeated by Sybil attack. This problem also occurs in distributed storage in wireless sensor network. In sensor network data is replicated and fragmented over several nodes but in reality data stored on malicious identities generated by the same Sybil node.

4.3 Data aggregation

In sensor network efficient query protocol is used for compute aggregated data to preserve energy rather than sending individual sensor reading. In sensor network some malicious node send incorrect sensor information might be unable to affect computed aggregated reading. However, in Sybil attack one malicious node may be able to participate to the aggregate many times. With enough Sybil nodes, an attacker completely alters the aggregate data.

4.4 Voting

Voting is used in wireless sensor network for different task. In Sybil attack the malicious nodes may be able to determining the outcome of any voting. Malicious nodes claim that misbehaviour in network done by legitimate node.

4.5 Fair Resource allocation

In some sensor network resources are distributed per node basis. A malicious node carried multiple identities can obtain an unfair share of any resources. Denial of Service may be caused to legitimate node by malicious node and allocate an attacker more resources to perform attack.

4.6 Misbehaviour Detection

In Sybil attack a malicious nodes could " spread the blame" by not having anyone Sybil identity misbehaviour enough for the system to take action. Sybil

Node, generate new identities nodes in network when action taken is to revoke the malicious node to never getting revoked himself.

5 DETECTION MECHANISMS OF SYBIL ATTACK

5.1 Resource Testing

Douceur in [2] proposed a resource testing approach to defend against the Sybil attack, which is based on the assumption that each physical entity is shortage in some resource. According to this approach communication,

computation and memory storage can be used for resource testing. In [10], Newsome et al. showed that computation and storage are not suitable to ad hoc networks,
because the malicious node can use more computational and memory storage resources than the legitimate node. As an alternative, they recommended a scheme based on radio resource testing. This scheme assumes that each node has only one radio which is not capable of sending or receiving on more than one channel, simultaneously. If a node wants to confirm the existing of Sybil nodes in its neighbors, it will allocate each of its neighbors a different channel to broadcast messages. The node then randomly choose a channel to listen. If the node hears the message on the channel allocated by the verifying node, then it is a legitimate node. Else, the neighboring node is treated as the Sybil node. However, how a sensor node allocating the radio channels to its neighbor nodes is an unsolved problem. In addition, this testing process may required a lots of battery power.

5.2 Random Key Pre-Distribution and Registration Based Key Validation

Newsome et al.[1] also projected a random key pre-distribution and registration based key validation method. In this method each node randomly picks '*n*' keys from a large pool of '*p*' keys. The number '*p*' is select such that two nodes will share at least one key with some probability after they pick their keys. The identity of the node is then pooled with the particular set of keys which it selected. In this way, any node can be authenticated by verifying some or all of the keys which it claims to acquire. But this process requires more memory space for storing pair wise keys with its neighbors. Moreover, if any malicious node is somehow able to take some keys, it can falsely claim the identities of many non-compromised nodes.

5.3 Trusted Base Station

Karlof & Wagner in [16] projected a protocol similar to Needham-Schroeder [10] to confirm the identities of two nodes. In this method a trusted base station acts as the Key Distribution Centre where all the nodes share their unique symmetric key. The base station then provides a shared key for each pair of nodes to verify each other's identity. This process can minimise the occurrence of the Sybil attack but cannot find out the location and eliminate it. If any malicious node succeeds in enter into network, and then it can create multiple fake identities to communicate with other nodes.

5.4 Location Based Cryptographic Keys

Zhang et al. in [5] introduced the concept of location-based cryptographic keys, called pairing. In this scheme, each node private key is combined with its ID and the geographic location. The Location-Based Keys(LBK) are generated using pairing based on identity based cryptography by a reliable authority. The protocol also includes a secure LBK-based neighborhood authentication scheme, and process for establishing both immediate and multihop pair wise shared keys. When a malicious node pretends to be a legitimate node, it does not have the valid LBK and thus, cannot effectively finish mutual authentication with other legitimate nodes. In the same way, a malicious node cannot claim fake IDs and locations without being detected. Therefore, the Sybil attack is successfully overcome. This method is not appropriate for large scale networks. Also, the pairing is an energy consuming method.

5.5 Network Coordinates

Bazzi et al. in [12] proposed a Sybil protection based on network coordinates in order to discriminate between nodes. The method relies on the hypothesis that a malicious user can have only one network position, defined in terms of its minimum latency to a set of beacons. In this process the node that wants to validate itself submits a geometric certificate consisting of verified ping times to a collection of standardized beacon nodes. Multiple virtual machines located at the same physical location will end up with essentially the same certificate, and can be treated as one (possibly corrupted) node. However, with network coordinates in a dimensional space, an adversary controlling more than d malicious nodes at d different network positions can fabricate an arbitrary number of network coordinates, and thus smash the defence. This mechanism is very difficult and energy consumptive.

5.6 RSSI(Received Signal Strength Indicator)

Demirbas and Song in [3] proposed Received Signal Strength Indicator (RSSI) based clarification to identify the Sybil attack in the wireless sensor networks. It is based on the fact that a malicious node with a number of fake IDs will have the similar signal strength. They showed that even though RSSI is unreliable and time varying in general and radio transmission is non-isotropic; using the ratio of RSSIs from multiple receivers it is possible to surmount these problems. The malicious node can vary its transmission power for its Sybil node leading to different received signal strength and hence erroneous detection of Sybil identities. This method is not appropriate for the MANETs, if the nodes go with non-uniform speeds.

5.7 TDOA(Time Difference of Arrival)

Wen et. al in [6] proposed a method similar to, based on the time difference of arrival (TDOA) between the beacon nodes and source nodes. This method requires at least three beacon nodes; one of them is the main beacon node and the others are called as inferior beacon nodes. When a malicious node broadcasts a message using one of its Sybil IDs, all the beacon nodes record the arrival time of this message, respectively. The inferior beacon nodes transmit their message arrival time information to the main beacon node. The main beacon node then computes the ratio of the difference of arrival time of the message at the inferior beacon nodes with respect to itself. Next time, if the same malicious node broadcasts another message with a different Sybil node, the above process of computing the ratio of time difference of arrival is repeated again. If this ratio is approximately same as that of the previous ratio, the Sybil attack is detected. But, this method is not suitable for the MANETs where the nodes move in different directions, with non-uniform speeds.

5.8 Mobility

Piro et al. in [8] proposed the mobility of nodes as a characteristic to detect the Sybil attack in MANETs. This method is based on the fact that all the Sybil nodes of a malicious node will always move together. If a set of nodes

are seen together for a long period of time by an observer node, then they are assumed to be the identities of Sybil attacker. The accurateness of the detection method can be further improved by using multiple confidential viewer nodes. However, this method fails if the malicious node continuously changes the identities of its Sybil nodes. Moreover, the confidential nodes can also be impersonated by the Sybil attacker node

5.9 Location Based Detection

Tangpong et al. in [13] used a location-based Sybil attack detection method for MANETs based on path similarity. The identities that go over the similar paths are considered Sybil nodes. Instead of selecting some confidential viewer nodes as in [8], each node in the network views and exchanges traffic study in order to analyze the potential existence of a Sybil attack. Moreover, to avoid a malicious node from fabricating with an study, a hop-byhop authentication protocols is being used.

5.10 Analyzing The Neighbouring Nodes

Ssu et al. in [9] used a detection method in which the node identities are confirmed simply by analyzing the neighboring node information of each node. This detection method is based on the fact that in a dense network, two different nodes cannot have the same set of neighbors. Because in a Sybil attack, all the Sybil nodes are created by the same malicious node, therefore, each of them will have same set of neighbors. This loophole of the Sybil nodes can be used to

detect the presence of a Sybil attack. However, this method is not suitable for mobile or semi mobile Ad hoc networks.

6 CONCLUSION

In this paper, we presented a brief survey on wireless sensor networks and security issues. Then we discussed one of the major attack- Sybil attack and

and establish a taxonomy of this attack**.** Sybil attack can extremely disrupt various operations of the wireless sensor networks such as voting, data aggregation, data replication and data fragmentation, fair resource allocation scheme, misbehavior detection and routing mechanisms. Then we have also discussed different techniques to alleviate Sybil attack.

REFERENCES

[1] J. Newsome, E. Shi, D. Song and A. Perrig(2004), "The sybil attack in sensor networks: analysis & defenses," in IPSN'04: Proceedings of the Third International Symposium on Information Processing in Sensor Networks**,** pp. 259–268.

[2] J. R. Douceur(2002), "The sybil attack", In IPTPS'01: Revised Papers from the First International Workshop on Peer-to-Peer Systems**,** pp.251–260.

[3] M. Demirbas and Y. W. Song(2006), "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", International Workshop on Wireless Mobile Multimedia**,** pp. 564-570.

[4] J. Wang, G. Yang, Y. Sun and S. Chen(2007), "Sybil Attack Detection Based on RSSI for Wireless Sensor Network", IEEE International Conference, pp. 684-687.

[5] Q. Zhang, P. Wang, D. S. Reeves and P. Ning(2005) "Defending against Sybil attack in sensor network", In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops(ICDCSW'05).

[6] W. Mi, L. Hui, Z. Yanfei and C. Kefei(2008), "TDOA-based Sybil Attack Detection Scheme for wireless Sensor Networks", Journal of Shangai University (English Edition), vol. 12, no. 1**,** pp. 66-70.

[7] J. Yang, Y. Chen and W. Trappe(2008), "Detecting Sybil Attacks in Wireless and Sensor Networks Using Cluster Analysis", IEEE International Conference**.**

[8] C. Piro, C. Shields, B. N. Levine, (2006), "Detecting the Sybil Attack in Mobile Ad-hoc Networks", *Securecomm and Workshops*, pp 1-11.

[9] K. -F. Ssu, W-T. Wang and W-C. Chang, (2009), "Detecting Sybil attacks in Wireless Sensor Networks using Neighboring Information", *Computer Networks*, vol. 53, (18), pp.3042-3056.

[10] R. Needham and M. Schroeder, (1978), "Using Encryption for Authentication in Large Networks of Computers", *Communications of ACM*.

[11] Y. C. Zhang, W. Liu, W. J. Lou and Y. G. Fang, (2006), "Location based compromise-tolerant security mechanisms for wireless sensor networks", *IEEE Journal on Selected Areas in Communications*, 24(2): pp. 247–260.

[12] Rida A. Bazzi, Young-ri Choi and Mohamed G. Gouda, (2009), "Hop chains: Secure routing and the establishment of distinct identities", *Theoretical Computer Science*, 410 (6-7): 467-480.

[13] A. Tangpong, G. Kesidis, H-Y. Hsu and A. Hurson, (2009), "Robust Sybil Detection for MANETs", *In Proceedings of the 18th International Conference on Computer Communications and Networks, IEEE ICCCN 2009*, San Francisco, California.

[14] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary(2007), "Wireless sensor network security – a survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press, .

[15] Jun Zheng and Abbas Jamalipour(2009), "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE.

[16] C. Karlof and D. Wagner, (2003), "Secure routing in wireless sensor networks: Attacks and Countermeasures", *Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, Vol. 1, No. 2-3, pp. 293-315.