Defense against Sybil attack in Wireless network using multichannel routing protocol

Ms. Damayanti R. Karale
Student: P. G. Dept. of Comp. Sci. & Engg.
SGBAU, Amravati
Maharashtra, India

Dr. Vilas M. Thakare
HOD: P. G. Dept. of Comp. Sci. & Engg.
SGBAU, Amravati
Maharashtra, India

Dr. Swati S. Sherekar
Prof.: P. G. Dept. of Comp. Sci. & Engg.
SGBAU, Amravati
Maharashtra, India

Abstract— *In the last decade, wireless ad hoc networks have emerged as a major next generation wireless networking technology. However, wireless ad-hoc networks are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most routing protocols assumes that there is no malicious intruder node in the network. Sybil attack is one of the serious attack at network layer, in which a malicious node poses as many identities in order to gain disproportionate influence. Node misbehavior due to selfish or malicious intention could significantly degrade the performance of wireless ad-hoc network because most existing routing protocols in wireless ad-hoc network are aiming at finding most efficiency path. In this paper, combining the two methods two detect and defense on the Sybil attacks is proposed. This proposed method is based on critical analysis. First method used to detect Sybil attack for multichannel wireless networks. This SybilCast protocol can ensure that each honest participant will receive at least a constant fraction for sharing the bandwidth with source node. It easily check the Sybil or malicious node and separate them. Finally the Mason test, to defense against the Sybil attack is present.*

Keywords— Wireless ad-hoc Network, Sybil attack, security, routing protocol.

I. INTRODUCTION

Wireless networking technology possesses numerous characteristics such as self-organization, flexibility, fault tolerance, high mobility, low cost and rapid deployment that make it ideal candidates for scenarios where certain network services such as secure message dissemination and event notification have to be provided quickly and dynamically without any centralized infrastructure [1]. The inherently vulnerable characteristics of wireless network, namely their unattended, and broadcast nature, appoint them vulnerable to various types of attacks [2]. A particularly harmful attack against ad hoc networks and sensor network is known as the Sybil attack, where an adversary creates multiple bogus identities to compromise the running of the system. The Sybil attack in which the legitimate node captured or an illegitimately node is inserted to the network by the adversary are called malicious nodes or identities. These nodes present multiple identities which are fabricated from the other legitimate nodes in the other parts of the network [3]. After the deployment of malicious nodes in the network topology, the nodes are presented a large number of Sybil ID and neighboring nodes think have many neighbor so the traffic of Sybil node is made traffic around themselves where it make be affected on routing protocol and some operation such as detection of misuse, data aggregation, etc. [4]. After the surveillance, with the high probability, attacker cannot produce false observation rate that make conforming identities look Sybil, due to the unpredictability of wireless channel [5].

In this paper, the SybilCast protocol are explore to give honest node for secure download the data. While most of the users are honest, some users may be malicious and attempt to obtain more than their fair share of the bandwidth. This is one possible strategy for attacking the system is to simulate multiple fake identities, each of which is given its own equal share of the bandwidth. Such an attack is often referred to as a Sybil attack. More specifically, protocol can ensure that each honest participant will receive at least a constant fraction for fair share of the bandwidth. This implies that each download of data will complete in asymptotically optimal time, even in the presence of a Sybil attack. The Mason test is a practical protocol for Sybil defense based on these idea. This test protocol have some requirement: conforming neighbors must be able to participate. That is, selective jamming of conforming identities must be detected. Probe packet must be transmitted in pseudorandom order. Moving node must be rejected. To save time and energy, conforming nodes that are moving when the protocol begins should not participate.

II. BACKGROUND

Security is most important thing in mobile sensor network, the sensor easily defeated by any attack, because of its have a broadcast nature. Sybil attack in one of the more known attacks on wireless sensor, which is identify and remove from the network gives the some detection and prevention

technique. The lightweight scheme is an accurate and practical algorithm to identify the Sybil node in mobile sensor node. This scheme eliminate the drawback of previous system. This scheme is based on the node mobility and it used the watchdog node for transmitting the data [1]. One more new scheme to detect Sybil attack in wireless sensor network using the UWB ranging-based information is proposed in [2]. It monitors and timely detects Sybil attacks in 802.15.4-like WSNs where the sensor nodes are randomly deployed in unknown position. The proposed ADS operates in a distributed manners, without depending on a third network entity. The obtained results show that Rulr-based anomaly detection system achieves high detection accuracy and low false alarm rate appointing it a promising ADS candidate for this class of wireless networks. The SybilCast is a new technique to detect a Sybil attack which in on multichannel wireless network is proposed in [3]. This protocol ensure that each honest participant will receive at least a constant fraction of his/her fair share of the bandwidth. This implies that each download of data will complete in asymptotically optimal time, even in the presence of a Sybil attack. The new Mason test is proposed in [4], which is used to defense against Sybil attacks and detect Sybil identities in wireless ad-hoc network and delay tolerant network without trusted authorities in any other node. In this method of O (n^3) complexity separate the true and false RSSI observation of behaving nodes from those falsified by malicious participants. Using the motion to defeat the signalprint technique attacker are detected by requiring low latency retransmission from the same position. This scheme gives the more than 99 percent eliminate the Sybil identities from the network. The scheme is to explore and dissect the procedure of carrying out sybil attacks in Opportunistic Networks [5]. In this scheme it identify the two main elements of a sybil attack such as link creation, ID fabrication and quantify the amount of effort and resources an adversary needs to spend on each of them. This is mainly due to the link formation mechanisms via high mobility, which demand continuous effort from an attacker.

This paper present brief introduction of Sybil attack defense techniques in **Section I**. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses Existing Methodologies. **Section V** analysis and discussion on existing techniques with Advantages & Disadvantages **Section VI**. Proposed methodology **section VII** possible outcomes and result and **section VIII** Conclude this review paper and Finally **Section IX** contains future scope for the current methodology.

III. Previous WORk Done

Rezvan. et al. (2014) [1] proposed a lightweight algorithm based on the context of node mobility, which is used to detect the Sybil in the mobile sensor networks. The proposed algorithm also used the watchdog node for identify the malicious node such as Sybil node which harmful to mobile sensor network. Communication overhead is the number of packets that the security algorithm is utilized to identify Sybil nodes in the network. The proposed algorithm is free the overhead due to one way communication between watchdog nodes and another nodes in the network and packet can be send to the sink node to identify the Sybil node. This method gives the 99 percent true result as compare to another method. This is more sophisticated network.

Panagiotis. et al. (2015)[2] proposed the rule-based anomaly detection system, called RADS, which monitors and timely detects Sybil attack in large-scale WSNs. The proposed system relies on an UWB ranging-based detection algorithm that operates in a distributed manner requiring no cooperation or information sharing between the sensor nodes in order to perform the anomaly detection tasks. The feasibility of the proposed approach is proven analytically. The obtained results shows that rule-based anomaly detection achieves high detection accuracy and low false alarm rate appointing it a promising ADS candidate for this class of wireless networks.

Zheng. et al.(2015) [3] proposed SybilCast protocol, this protocol is used for multichannel wireless networks that limits the number of fake identities and ensures that each honest user gets at least a constant fraction of his or her fair share of the bandwidth. It provides asymptotically optimal transmission speed for honest nodes. The strategy used in this article to detect Sybil identities is one variant of simultaneous receiver test.

Yue Liu. et al. (2015)[4] proposed a two methods for separating the valid RSSI observation of behaving nodes from those falsified by malicious participant nodes. Further proposed and Mason test to detect Sybil attacks in open ad-hoc network and delay tolerant network without requiring trust in any other nodes or authority. The Mason test implemented in both indoor and outdoor environment and proposed protocol is usable, safe, and secure.

Trifunovic, Andreea Hossmann-Picu et al. (2014)[5] proposed method is an analysis based method it shows that the types and effectiveness of Sybil attacks that are possible in opportunistic network, under various resource constraints on the attacker. In this method it identify the two main elements of Sybil attack link creation and ID fabrication and quantify the amount of efforts and resources an adversary needs to spend on each of them.

IV. Existing Methodology

A. Detection of Sybil nodes in Mobile sensor networks Using the context of nodes mobility:

It is lightweight algorithm based on the context of node mobility, which is used to detect the Sybil in

the mobile sensor networks. In this algorithm, considered the special case of Sybil attack where malicious node attempts to be selected as the cluster heads in LEACH and the Sybil nodes are detected by the base station. So the false detection rate in this algorithm is lower than the other algorithms [1].

B. Detection of Sybil attacks in wireless sensor networks Using UWB ranging based information:

This scheme based on rule-based anomaly detection system, called RADS, which monitors and timely detects Sybil attack in large-scale WSNs. The proposed expert system relies on an ultra-wideband ranging-based detection algorithm that operates in a distributed manner requiring no cooperation or information sharing between the sensor nodes in order to perform the anomaly detection tasks. The applied architecture is considered as cost-effective, since no high-cost hardware is used and there is no need for additional base station existence [2]. Determine the probability density function of a single node n_i to have exactly x neighbors. By considering that M total nodes are uniformly distributed in a sensor field of area E, the probability $q^i(x)$,0<=x<=M-1, is derived as follows:

$$q^i(x) = Pr(X = x) = \binom{M-1}{x} \alpha^x (1-\alpha)^{M-(x+1)}$$

where a α<= 1 denotes the geometric probability of node nj to be within the communication radius R of node ni, where ni – nj. This probability is given by:

$$\alpha = \frac{\text{Area of favorable region}}{\text{Area of total region}} = \frac{\pi R^2}{E}, \quad \pi R^2 \leqslant E$$

C. SybilCast protocol to detect Sybil attack in multichannel:

The SybilCast protocol is used to check the Sybil attack in wireless network with multiple channel based [3]. This protocol limits the maximum number of fake identities or Sybil identities and provides asymptotically optimal transmission speed for honest or legitimate nodes. It ensures that each honest node or users gets at least a constant fraction of his or her fair share of the bandwidth. The main idea behind this protocol is balancing the rate at which new identities and nodes are admitted and the maximum number of fake identities that can coexist while keeping the overhead low [3]

D. The Mason test defense against Sybil attack:

It is the new defense technique against Sybil attack in wireless network. In this scheme first separate the all legitimate node and illegitimate node through RSSI observation. Apply the challenge response protocol to detect attackers attempting to use motion to defeat the signal print based Sybil defenses. Once the all nodes are separated apply the Mason test, it is a practical protocol for Sybil defenses based on these idea. This protocol is based on the pre-signed message and communicate one node to another node through faster secret-key schemes, which is easily detect the legitimate node and destroyed the illegitimate node. This scheme gives the high computation time with high false positive rates [4]. At least one is still conforming with high probability:

$$1 - \left(1 - \prod_{m=2}^{n-1} \frac{(1-\gamma_m)\cdot|C| - (m-1)}{|LNS| + (1-\gamma_m)\cdot|C| - (m-1)}\right)^{|C|}.$$

E. Stalk Me if You Can- the Anatomy of Sybil attacks in Opportunistic Networks:

This scheme show that the limits of the sybil attack in terms of general trust establishment, which is an important first step, there is much more to explore, such as Sybil's' impact on routing specific metrics. The opportunistic network are highly distributed and dynamic in nature makes them easy targets for Sybil attack [5].

V. Analysis And Discussion

Security is the major concern in wireless ad-hoc network, there are many existing technique to detect any defense against the Sybil attack. Sybil attack one of the most harmful attack, which cannot detected easily in wireless network. Multichannel based protocols are easily help to detect the Sybil attack in network. The SybilCast protocol is used to detect Sybil attack at multichannel level, which takes any many number of channel for sending and downloading the data. This is an efficient and robust protocol that can be let the base station deliver the requested data to all active honest nodes. This is fair share protocol for communication between server and client node.

The SybilCast protocol can efficiently detect the Sybil identities with lower overhead than the previous radio resources testing algorithm. It is good steady state constraint on the number of Sybil identities, because it balancing the admission rate and the detection rate. This protocol eliminate the Sybil identities at constant bandwidth [3].

The Mason test protocol for defense against Sybil attack. This protocol uses the secret key for sending the packet from one station to client node. This method is used both indoor and outdoor type network. An attacker could theoretically improves its collapsing probability by pre-characterization the wireless network topology. There is vast majority of rejected conforming nodes were eliminated due to motion [4].

TABLE 1: COMPARISONS BETWEEN EXISTING SYSTEM METHODS

Segmentation Techniques	Advantage	Disadvantage
SybilCast protocol to detect Sybil attack in multichannel	It is a randomized protocol, hence all its guarantees hold with high probability	The parameter are not well optimized for better performance purpose.
The Mason test defense against Sybil attack	It implemented in both indoor and outdoor environment. The proposed protocol is usable, safe, and secure.	It have limited ability to predict the RSSI observation of the node.
Detection of Sybil nodes in Mobile sensor networks Using the context of nodes mobility	false detection rate in this algorithm is lower than the other algorithms	When a node finds this information that one or more than intermediate nodes are not supporting in the packet forwarding.
Detecting Sybil attacks in wireless sensor networks Using UWB ranging based information	RADS does not require cryptography methods	The detection of indirect Sybil attacks is not supported by the proposed system
Stalk Me if You Can- the Anatomy of Sybil attacks in Opportunistic Networks	This methods are highly distributed and dynamic in nature makes them easy targets for Sybil attack.	This approach is difficult to implement and not very effective.

VI. Proposed Methodology

Malicious user detection is primary policy of the network designer; in this multichannel routing protocol is used to detect the malicious node from the network and discard it. The multichannel routing protocol in this consider a synchronous wireless network consisting of one base station and a dynamically changing set of clients. There are at most N clients, an unknown subset of which are active at any given time for communication. If there is no confusion, then call these clients wireless node. Each node may either be an honest node or a malicious node. If the client nodes are active they start the communication with base station through multichannel wireless radio network. Assuming here a reasonably large number of available channels. Every node i.e. honest node or malicious node and the base station have a one radio transceiver. Time is divided into rounds and each node and the base station can access the only one channel in each round. The first round is registration, where new nodes enter the system and request for registration after registration it gives the unique and random binary string to each new request node. And also verify and detect all the nodes and eliminate malicious node or Sybil node. In this phase each registered identity should transmit a verification message to base station for confirmation. The base station receive and verify these message and remove node that fail to send verification message. Then it goes through the data phase is used to transmit data packets and deliver authentication message from the base station to the registered identities. In each round the data phase the base station randomly chooses the registered identity and sends it a packet on the channel. This show that all malicious node are eliminate and honest node for further process.

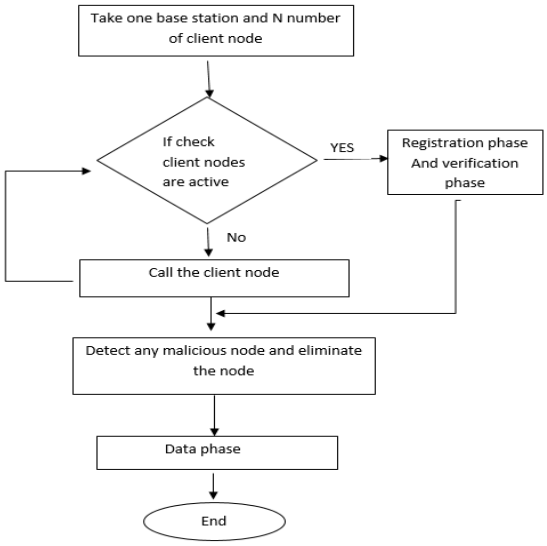

Fig 1: Flowchart for multichannel protocol

Mason test protocol: This protocol requires four main requirement.

I. Conforming neighbor's nodes must be able to participate. It means selective jamming of these identities must be detectable.
II. Review packets must be transferred in pseudorandom order. Further, each member must be able to validate that no set of identities controlled the order.
III. Moving nodes must be rejected in order to save energy and time. The protocol should not participate when the nodes are moving initially.
IV. When the attacker constructing fake values, he must not know the RSSI observations of the conforming nodes.

VII. Possible Outcome And Result

The proposed multichannel routing protocol is used to detect the Sybil identities or malicious identities from the given network with lower head as compare to previous resource testing protocols. This is more efficient and robust method for detection. And it also provide some defense

mechanism on it. This protocol have high performance accuracy and detection policy. In this protocol uses three phases for secure communication between base station and client nodes. Multichannel wireless radio is to detect all the enter client node, if more than one node take one channel at a time the base station will be destroyed the node information and does not allow it for again to enter in the network topology. In Mason test probe packet must be transmitted in pseudorandom order. Moving node must be rejected. To save energy and time, conforming nodes that are moving when the protocol begins should not participate. The transmission bandwidth for each and every node is same.

VIII. Conclusion

In this paper, described a method to detect the Sybil attacks in multichannel wireless ad-hoc network. And can be differentiated between honest node and dishonest node with optimal transmission speed for honest nodes. The protocol that achieve both fairness and asymptotically optimal throughput in the presence of Sybil identities. Most of the time location will be free for such attackers, the Mason test provides a way to verify this condition, reject any Sybil and let other protocol operate knowing they are Sybil free. The vast majority of rejected conforming nodes were eliminated due to motion. These methods are also widely used in security mechanisms as they are adaptable to dynamic changes in the real world network conditions. This is the theoretically based concept.

IX. Future Scope

Further improve the accuracy and reduce the error rate and link failure. It will be help to improve the high security system.

Acknowledgment

I, Damayanti R. Karale, thankful of my supervisor Dr. V. M. Thakare and Professor Dr. S. S. Sherekar for helping to complete this research paper.

References

[1] Rezvan Almas-Shehni, and Karim Faez," Detection of Sybil Nodes in Mobile Sensor Networks Using the Context of Nodes Mobility," Springer International Publishing, pp 117-128, 2014.

[2] Panagiotis Sarigiannidis, Eirini Karapistoli Anastasios A. Economides," Detecting Sybil attacks in wireless Sensor Networks Using UWB ranging- based information," Elsevier Expert Systems with Applications, Vol 42, pp 7560-7572, June 2015.

[3] SETH GILBERT and CHAODONG ZHENG," Sybil Cast: Broadcast on the Open Airwaves," ACM Transactions on Parallel Computing, Vol. 2, No. 3, PP 16:1-16:20, September 2015.

[4] Yue Liu, David R. Bild, Robert P. Dick, Z. Morley, Mao, and Dan S. Wallach," The Mason Test: A Defense Against Sybil Attacks in Wireless Networks without Trusted Authorities,"IEEE TRANSACTIONS ON MOBILE COMPUTING, vol. 14, no. 11, pp 2376-2390, November 2015.

Sascha Trifunovic, Andreea Hossmann-Picu," Stalk Me if You Can – The Anatomy of Sybil Attacks in Opportunistic Networks," ACM Journal, pp 37-42, September 2014.