International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 7|| July 2017 || PP. 43-48

Impact Evaluation of Sybil Attack on Manet's for Reactive Routing Protocol

Gurkirat kaur
Department of CSE
Baba Banda Singh Bahadur Engineering College

ABSTRACT *: A number of attacks have to be faced by mobile ad hoc networks like sybil attack. In the present this as well, the focus is on the practical evaluation of effective way to detect and prevent a Sybil attack. When a Sybil attack, the reputation system of current work is subverted by generating a large number of fake identities and these are used to achieve disproportionately large influence on the network. A Sybil attack is dangerous for security as well as the trust of the network. In this case, the running of the network is compromised. There are several methods that have been offered earlier by various researchers for the purpose of mitigating Sybil attack from MANET that all of these and have their individual benefits and limitations. In the present research work, first of all, we are going to detect the Sybil attack and then to prevent the attack in order to uphold the overall performance of the network. In the present research work, the method being investigated is based on three step algorithm: (i) monitoring (ii) trust value; and (iii) isolation. First of all, the nodes in the network will be monitored and then maintained trust value will be used to differentiate between legitimate and Sybil node, and in the end, the Sybil node will be isolated from the network. This work will be practically evaluated by using network stimulator (NS2) by evaluating throughput, end-to-end delay and packet delivery ratio in case of various network conditions.*

KEYWORDS - *Mobile Ad hoc Network, Packet Delivery Ratio,Sybil Attack,Trust Value.*

I. INTRODUCTION

The Mobile Ad Hoc Networks (MANETS) comprises of mobile, reader devices over wireless communication channel. This type of network does not need any fixed infrastructure and data communication or routing is done as and when needed. They are decentralized and autonomous wireless systems. MANETS comprises of mobile nodes that are free in moving in and out of the network. MANETS have become the center of attraction as a result of their promising and interesting functionalities which include mobile safety, location-based services and avoidance of traffic congestion. In case of Mobile Ad Hoc Network, security is most significant concern regarding basic functionality of network. The availability of network services, integrity and confidentiality of data can be achieved by making sure that security issues are fulfilled. Generally MANET had to face security attacks as a result of their features like open medium, lack of central monitoring and management, changing its topology dynamically, cooperative algorithms and lack of a clear defense mechanism [1] . MANET also becomes more vulnerable to security attacks due to wireless links as a result of which it becomes easier for the attackers to go inside the network and access ongoing communication. The mobile nodes that exist within the range of network link can overhear and even take part in the network. The framework that is going to be developed in this research work is based on the trust value of each node. In case of this technique, there is a server in the network, which monitors each node and keeps track of the overall history of all the nodes dynamically in order to know regarding them. Hence, when there is a small change in the behavior of any node, the server comes to know that the particular note is misbehaving or it is a malicious node. Therefore the server can isolate it. From the network. There is no need for any extra hardware in case of this technique.

We are aware that in MANET, the communication takes place on mutual trust between the nodes, and there is no central point for network management or any authorization facility, vigorously altering the polity and limited resources. Such networks are particularly vulnerable to various types of attacks like a black hole attack, Sybil attack, black hole attack, routing table overflow attack, flooding attack or denial of service (DoS) [2]. In the present research work, the main focus will be on detection and prevention of a Sybil attack and the other types of it did not fall within the review of this research work. A Sybil attack can be described as a situation where a malicious node behaves like two or more nodes. Instead of just one node like earlier mentioned attacks [2]. The Sybil, nodes are generated by its series of false identities, imitations or the importance of mission of nodes present in MANET and the identities of these additional nodes can be created by just one physical device. This

attack results in danger for the basic functionalities of MANETs. Hence, a secure method is required, that is not only capable of detecting a Sybil attack, but is also capable of preventing the attack from causing a significant damage to the network.

In the present research work, another strategy is being introduced alongside its pragmatic examination for recognizing and avoiding Sybil attack productively in MANET. If there should arise an occurrence of this technique, trust esteem is utilized for separating between Sybil node and authentic node. In different parts of this research paper, Section 2 shows the writing review. Segment 3 of the paper examines the approach explored and its calculation. In area 4, the outcomes are talked about lastly in segment 5, conclusion is introduced.

II. LITERATURE SURVEY

A related monetary investigation of lightweight Sybil assault recognition Theme in portable impromptu networks has been proposed by Mulla [1]. The creator has assessed this system utilizing network stimulator-2. The sensible examination of the procedure is finished by considering the network conditions like customary network conduct, the nearness of Sybil Cretan hubs in Cretan network and in the end arranged approach to find sensible assailants in the network. The execution correlation is finished between three assortments of network conditions with a view to accomplish execution of arranged system is closely resembling conventional network condition. The outcomes influences it to clear with RSS, even with Sybil aggressors, the approach being researched works effectively and does not bring about any loss of information. The main impediment give this system is that top of the line to end postpone as against customary network condition.

Kasiran et al. [2] has evaluated the turnout of AODV beneath in spite of the fact that and Sybil assault. In this research work, the creator has assessed the turnout execution in AODV with the nearness of empty and Sybil assault. It is uncovered by the recreation result that there is refinement execution thus out at whatever point there is a partner assault. It is likewise uncovered by the execution investigation that the turnout basically diminishes if there should arise an occurrence of empty assault and Sybil assault than in the event of the nonappearance of such a hub.

Patidar et al. [3] had altered the directing instrument of AODV for impedance against dark gap and warmth opening assault. In this work, conventions have been recommended that can guard improvised systems from dark opening and empty assaults and furthermore to increase the strength of the system. A partner interruption, refering to framework has been introduced in this paper, and it underpins the prospect of determination based location is done keeping in mind the end goal to recognize and thwart blackhole assaults. Additionally, in this paper, a jump check examination approach has likewise been exhibited to locate all of assaults on courses in extemporaneous system. The anticipated convention does not require any area information, time synchronization or any exceptional equipment for finding empty assaults. Tuned in to the recreation comes about, the task the strategy stays predominant execution as PDR and expanded turnout, however normal end to end defer likewise increments.

Liu et al. [5] has found a method to use signal prints for the purpose of detecting Sybil attacks in open ad hoc and delay tolerant networks without needing trust in any other node or authority. The inherent difficulty present in predicting RSSI has been used by this paper to separate true and false RSSI observations that are reported by one hop neighbors. The attackers that use motion to defeat the signal prints technique are discovered by requiring low latency retransmissions from same position.

A method has been proposed by Feng et al. [6] for safeguarding against multisource Sybil assaults in VANET. In this work, the creator has proposed an event-based reputation system (EBRS). For this situation, dynamic notoriety and trust and incentive for every occasion are utilized to stifle the different of false message. EBRS is fit for distinguishing Sybil assault where created personalities and stolen characters in procedure of correspondence. It can likewise shield against planned Sybil assault in light of the fact that for this situation, every occasion has novel notoriety esteem and put stock in esteem.

III. METHODOLOGY INVESTIGATED

In this area we are showing our proposed strategy for identifying and forestalling sybil attack. This strategy does not require any additional equipment or anything for its execution.Below are listed the main 3 steps of this method and the flowchart presented in figure 1.

Step 1. Monitoring :In this step, a server is broadcasting the hello packets in the network to monitor the network nodes. The role of hello packet is to check the node position, node ID, node neighbours and energy. The hello packets fetch the information regarding the nodes to the server. The fetched information is used to maintain the routing tables in the networks. Now we have a routing table and the server is regularly monitoring the network nodes to check the trust value of each node. The proposed method uses DSR protocol's routing table for monitoring of nodes.

Step 2. Trusted : During this step, the trust value table is maintained in the network to identify whether a node is legitimate or a malicious node. The trust value table is maintained by the server where initially all the nodes are rewarded with a 0 trust value. As the network starts to send packets. For each successful transmission, a node is rewarded with a trust value point. If the node sends the packet to the wrong destination then it is given a negative point. The server is dynamically setting up a trust threshold value. The major role of this step is to compare the trust value of the node with the trust threshold value. If the value is greater than or equal to the threshold value ,then the node marked as legit node otherwise it is marked as sybil node.
Step 3. Isolation : In the proposed method we use the multiple path method to prevent sybil attack i.e the network maintain multiple path between source and destination and initially the packet is forwarded on the most optimal path in case, a malicious node is present in the path. The network adopt another secured path. It may be a second optimal path. During this step, nodes must be enable or capable of adopting changes in the network. The nodes which are detected are sybil or attacker nodes are isolated from the network and the paths are deleted from the network.

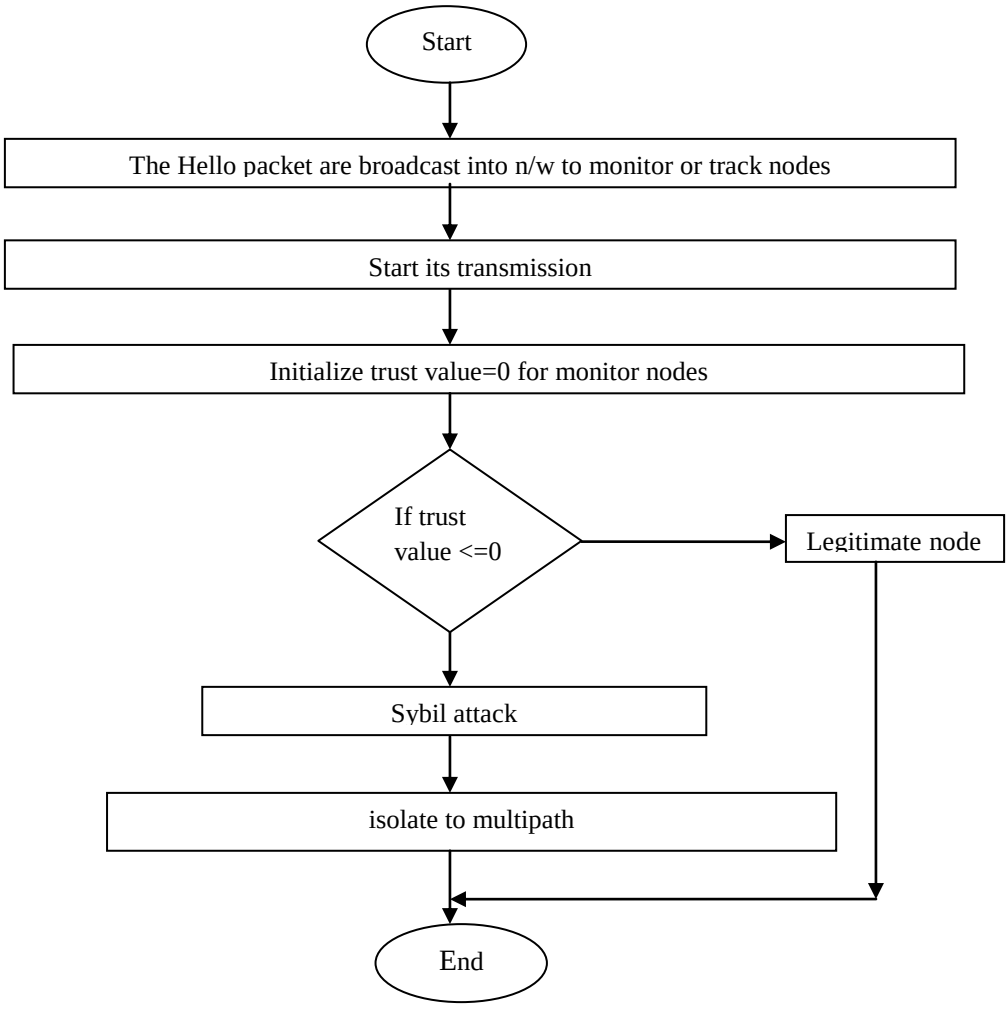

Figure 1: Flow-chart of the proposed method

Below is the algorithm of the proposed method.
Algorithm:
Step 1: Start Hello packet are broadcast into network to monitor nodes.
Step 2: Start transmission of packets in a network.
Step 3: Initialize the counter in routing table.

```
If(sod==true)          //source to destination packet successfully sent.
    Counter++;
Else
    Counter--;
```

Step 4: Initialize the trust value then compare this value with counter and detect the Sybil attack.

```
If(trust value<=0)
```

```
        Sybil attack
    Else
        Legitimate node
```

Step 5: Isolate to multipath.

```
If(trust value <0)
    Multipath                //it may  change the path
Else
    Legitimate node          // same  path use.
```

Step 6: End.

Our arrangement influences utilization of the trust to an incentive to recognize an honest hub and sybil hub and after that in the long run disengaging the sybil character from the system.

IV. PRACTICAL RESULTS AND ANALYSIS

In this segment we are talking about the tool used, network configuration parameters, performance metrics, and the results obtained.

4.1 Tool Used:

Network Simulator-2 is utilized to complete the recreation. NS-2 give innovations, protocols,communication gadgets for scholarly research, evaluation and change. It is productive, strong and exceptionally dependable which give the client the simplicity of graphical interface, creating and running the recreation and approval of the outcomes.

4.2 Network Configuration Parameters:

The proposed method uses the following network configuration parameters :

Table 1: Network Configuration Parameters

Number of Nodes	30
Traffic Patterns	CBR(constant Bit Rate)
Network Size(X*Y)	1000*1000
Max Speed	2/4/6/8/10/12/14/16 m/s
Simulation Time	100s
Transmission Packet rate time	10m/s
Pause time	1.0s
Routing Protocol	DSR, Sybil-DSR,IRS-DSR
MAC protocol	802.11

4.3 Performance Metrics:

1. PDR vs. node speed
2. End to End Delay vs. node speed
3. Average Throughput vs. node speed

4.4 Results Obtained:

For the proposed work, following are the three graphs demonstrating the execution of proposed strategy comes about:

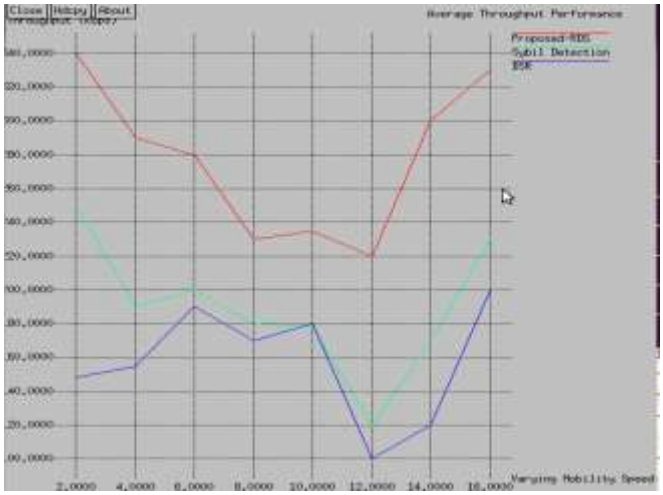

Figure 2:Performance of Average Throughput Analysis

The comparison of figure 2 shows that increasing speed the Delay of proposed technique is less than previous technique. The comparison shows the proposed technique has better results in varying speed environment Delay performance as compared to previous technique.

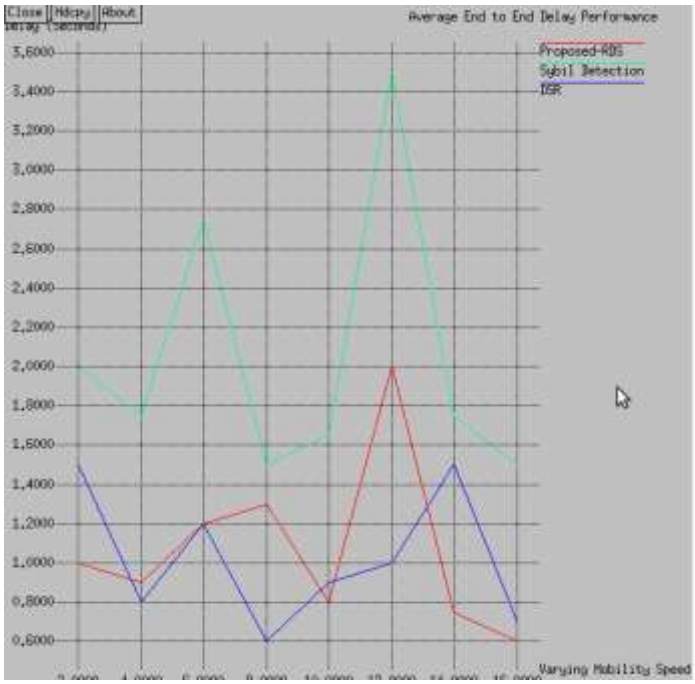

Figure 3:Delay Performance Analysis

From the above graph it demonstrates that end to end delay is lesser in trust esteem based technique.

Figure 4: Performance of PDR (%) Analysis

The comparison of figure 4 shows that increasing speed the PDR of proposed technique is higher than previous technique. The comparison shows the proposed technique has better results in varying speed environment for Packet Delivery Ratio as compared to previous technique.

From the above graphs we infer that , the researched trust esteem based technique accomplishes better execution for sybil attack discovery and counteractive action. This approach not just recognizes the sybil attack and give security yet additionally keeps it from creating any hinderance in the working of the system.

V. CONCLUSION

In this paper we laid out trust esteem based technique for sybil attack location and avoidance in MANETs. In the present work the trust based scheme is used to detect the sybil attack. The existing RSSI based method of detecting sybil attack is less effective as malicious paths are often used, where as present work is adopting multipath method to avoid such paths. The trust scheme ensure the reliability of the source and destination. The continuous monitoring of nodes behaviour is regularly used to update trust value. The proposed work is done using Network Simulator-2. The performance of proposed work is evaluated on basis of various performance parameters like delay and packet delivery ratio. The present work shows quite improved results. In future, an authentication module may be coupled with trust base scheme , which immune network against other attacks too.

References

[1] M. Mulla, "Efficient Analysis of Lightweight Sybil Attack Detection Scheme in Mobile Ad hoc Networks," in *IEEE 2015 International Coference on Pervasive Computing*, 2015.

[2] Z. Kasiran and J. Mohamad, "Throughput performance analysis of the wormhole and sybil attack in AODV," in *IEEE 2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2014, pp. 81–84.

[3] K. Patidar and V. Dubey, "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 54, no. 7, 2014.

[4] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi, "SoK: The evolution of sybil defense via social networks," *Proc. - IEEE Symp. Secur. Priv.*, vol. 21, no. 2, pp. 382–396, 2013.

[5] Y. Liu, D. R. Bild, R. P. Dick, Z. M. Mao, and D. S. Wallach, "The mason test: A defense against sybil attacks in wireless networks without trusted authorities," *IEEE Trans. Mob. Comput.*, vol. 14, no. 11, pp. 2376–2391, 2015.

[6] X. Feng, C. Li, D. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Springer Peer-to-Peer Netw. Appl.*, vol. 1, no. 9, 2016.

[7] G. Garg, S. Kaushal, and A. Sharma, "Reactive Protocols Analysis with Warmhole Attack in Ad-hoc Networks," in *IEEE ICCCNT 2014*, 2014, no. 1, pp. 1–5.

[8] J. Biswas, A. Gupta, and D. Singh, "WADP : A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol," in *Springer Information Communication and Embedded Systems*, 2008, pp. 1078–1085.

[9] S. Ji, T. Chen, S. Zhong, and S. Kak, "DAWN: Defending against wormhole attacks in wireless network coding systems," *INFOCOM, 2014 Proc. IEEE*, pp. 664–672, 2014.

[10] C. B. Dutta and U. Biswas, "Specification based IDS for Camouflaging Wormhole Attack in OLSR," in *IEEE 2015 23rd Mediterranean Conferance on Control and Automation (MED)*, 2015, pp. 960–966.

[11] Z. Han, L. Lu, and M. J. Hussain, "Real-time and Passive Wormhole Detection for Wireless Sensor Networks," in *IEEE 2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2014, pp. 978–985.

[12] P. Lee, S. Member, A. Clark, S. Member, L. Bushnell, and S. Member, "A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems," *IEEE Trans. Autom.Control*, vol. 59, no. 12, pp. 3224–3237, 2014.

[13] A. Patel, N. Patel, and R. Patel, "Defending against Wormhole Attack in MANET," in *IEEE 2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp.674–678.

[14] J. Anju and C. N. Sminesh, "An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET," in *IEEE 2014 3rd International Conference on Eco-friendly Computing and Communication Systems*, 2014, pp. 149–154.

[15] V. Teotia and I. Woungang, "Wormhole Prevention using COTA Mechanism in Position Based Environment over MANETs," in *IEEE ICC 2015- Communication Software, Services and Multimedia Applications Symposium*, 2015, pp. 8664–8668.

[16] D. Aldhobaiban, K. Elleithy, and L. Almazaydeh, "Prevention of Wormhole Attacks in Wireless Sensor Networks," in *IEEE 2014 2nd International Conference on Artificial Intelligence, Modelling and Simulation*, 2014, pp. 287–291.