Intrusion Response System of Sybil Attack using DSR Protocol in MANET

Manpreet Kaur
M.Tech Student
Department of Computer Engineering, YCOE
Pbi. University, Patiala Guru Kashi Campus,
Talwandi Sabo

Manoj Kumar
Assistant Professor
Department of Computer Engineering, YCOE,
Pbi. University, Patiala Guru Kashi Campus,
Talwandi Sabo

ABSTRACT
MANET is infrastructure less and independent network which consists various nodes. MANET is mobile ad hoc network having ability to connect various mobile nodes to each other. These nodes use wireless links to communicate with each other. In this paper, main aiming to present practical evaluation of efficient method for preventing and detecting Sybil attack. Sybil attack is an attack which uses several identities at a time and increases lot of misjudgments among the nodes of a network or it may use identity of other legitimate nodes present in the network and creates false expression of that node in the network. Like this, it disturbs the communication among the nodes of the network. This kind of attack results into major information loss and hence misinterpretation in the network, it also minimizes the trustworthiness among mobile nodes, data routing disturbing with aim of dropping them in n/w etc. There are many methods previously presented by different researchers with aim of mitigating such attacks from MANET with their own advantages and disadvantages. this paper is introducing the study of Intrusion Response System for lightweight Sybil attack using DSR in MANET. The practical analysis of this work is done using Network Simulator (NS2) by measuring throughput, end to end delay and packet delivery ratio under different network conditions.

Keywords
MANET, Sybil attack, DSR, NS2, Throughput, end to end delay, PDR

1. INTRODUCTION
MANET is infrastructure less and self-configurable network wherever varied users will communicate on temporary basis. It's assortment of nodes that communicate with one another by the wireless links.

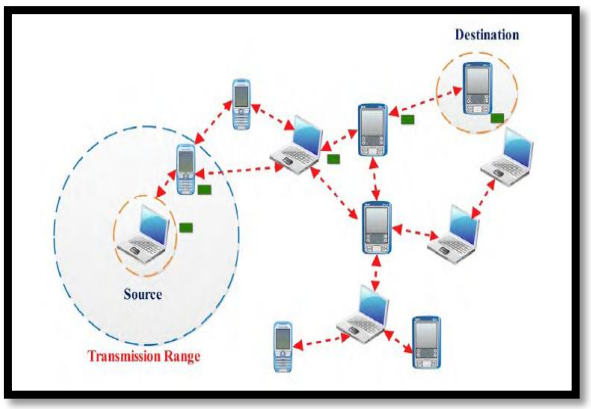

Fig.1: Mobile Ad hoc Network

Due to infrastructure less nature of MANET and as there is no central authority to maintain and control the network makes it vulnerable to various attacks.

Sybil attack is an attack which uses several identities at a time and increases lot of misjudgments among the nodes of a network or it may use identity of other legitimate nodes present in the network and creates false expression of that node in the network. Like this, it disturbs the communication among the nodes of the network. To have secure communication it is necessary to eliminate the Sybil nodes from the network.

As familiar to MANET which consists of mobile, radio devices over the wireless communication channel. This network does not require any fixed infrastructure and data communication or routing done as and when required. However these types of networks are vulnerable to different kinds of security attacks such as wormhole, black hole, Sybil attacks etc. The main focus of this paper is on Sybil attack detection, other kinds of attacks are out of scope of this paper. In MANET, Sybil attacker damage MANETs in

Many ways . Hence such kind of attacks will have danger causes on the basic functionalities of wireless networks. Therefore once needs to have strong secure method which can not only identify such attackers in MANET but also mitigate them from causing serious damage in networks. The previous methods for preventing the Sybil attacks are based on use of cryptographic based or trusted certification based authentication. The limitation of this method is that it needs costly startup setup and also resulted into extra overhead in order to maintaining as well as distributing cryptographic keys. Other than this, some methods introduced were based on use of RSS for identifying the Sybil attackers in MANETs. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc network. However, this approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS) [1].

During this paper we are presenting new method and its practical analysis to detect and prevent Sybil attacks in MANET efficiently as compared to previous methods. This method uses trust value for differentiating identities of Sybil node and legitimate node. Rest of paper divided into below points. In section II, the related work presented. In section III, the method and its algorithm is presented which we are taking here for investigation and practical analysis. In section IV, results are discussed using NS2; finally conclusion is presented in section V.

2. RELATED WORK

Sybil attack was first introduced by Douceur. According to Douceur [2] there is no practical solution for this attack. Deploying Trusted Certification is the only scheme that can completely eliminate the Sybil attack. However, it suffers from costly initial setup, lack of scalability and a single point of attack or failure. Also, it's based on the assumption that each entity has single identity which is very difficult to achieve on the large network. Pareek and Sharma[3] proposed the Sybil Attack Detection technique which is used to detect the Sybil nodes in the network and also prevent it. This paper propose detection of Sybil attack is finished by victimization MAC address. Analysis had done by some answer that features the communication among the nodes of cluster. Analysing the leads to numerous situations like pretend sender detection and pretend receiver interference and node to node secure association and packet acceptance and rejection method. **Elboukhari et al.** [4] had addressed MANETs are more vulnerable to attacks because they have some specific characteristics as complexity of wireless communication and lack of infrastructure. Hence security is an important requirement in mobile ad hoc networks. In this paper we investigated the impacts of attacks on the network performance. simulated black hole attacks using Network Simulator 2 (NS-2) and have measured the packet loss in the network without and with a black hole attacks. Also, wemeasured the packet loss when the number of black hole attacks increases. **Patidar & Dubey [5]** had proposed changed the routing mechanism of AODV for interference against Black and heat hole attack. The paper proposes protocols which might defend impromptu networks from blackhole and hollow attacks and to spice up network stability. This paper presents associate intrusion observance system supported the thought of specification-based discoverion system to detect and forestall blackhole attacks. This paper to boot presents a hop count analysis approach to sight hollow attacks on routes in impromptu networks. The projected protocol does not would like any location data, time synchronization, or special hardware to sight hollow attacks. in step with simulation results the projected techniques show superior performance as PDR and turnout can increase however, average end-to-end delay to boot can increase. among the analyzed scenario, it's found that the modified AODV and IDS-AODV has superior performance than AODV. **Kasiran and Mohamad [6]** had proposed Throughput performance Analysis of Warmhole amd Sybil Attack in ADOV. In order to communicate each other, the nodes cooperatively forward data packets to other nodes in the network by using the routing protocol. However, these routing protocols are not secure hence leaving the MANET unprotected from malicious attack. Wormhole attack is a common malicious attack in MANET environment. The network consisting of 20, 60 and 100 mobile nodes uses the random model in 1000m x 1000m flat area. The sources are spread randomly over the network and only 512 bytes data packets are used. Each packet is uniformly dispersed at 180 sec, starting its journey from a random location to a random destination the objective of this paper is to evaluate the throughput performance in AODV with the existence of wormhole and Sybil attack. The simulation result has shown that there is difference performance in throughput when there is an attack. **Feng, Li, Chen, and Tang [7]** projected a way for defencing against multi-source Sybil attacks in VANET. During this paper, author propose an occasion based name system (EBRS), throughout that dynamic name and trustworthy price for each event are used to suppress the unfold of false messages. **Biswas, Gupta and Singh [8]** had projected hollow Attack Detection And interference Technique in Edouard MANET victimization modified AODV routing Protocol. Author proposes associate rule to sight wormholes with none special hardware. **Aldhobaiban, Elleithy and Almazaydeh [9]** advised the foundations for interference of hollow Attacks in Wireless detector Networks. **Dutta & Biswas [10]** had analysis impact of warmth hole attack on OLSR routing protocol . A modified version of hollow attack is developed throughout this paper, noted as camouflaging hollow attack, and a corresponding specification primarily based wholly IDS is supposed to sight and forestall this attack.

3. PROPOSED TECHNIQUE FOR DETECTION & PREVENTION

In this proposed a method some selecting neighbors are participating in detecting Sybil attack. The neighbors are selected in random ways. They are also altered about Sybil attack.

This method firstly packets are broadcast into network to monitoring the nodes of network. Then compare the trust value into routing table and detect to Sybil attack based on trust value. If Sybil attack is detected into network then trust node inform about it may be an attacker. Then it may be path change for transmission.

3.1 Proposed Method

The proposed method for detecting and preventing Sybil attack using DSR protocol uses mainly three steps:

Step 1: Monitoring

In this step, This method start Hello packets are broadcast into network to monitor nodes. After broadcasting, transmission of packets in a network are started. Then trust node track to nodes in network. The proposed method used DSR protocol's routing table for monitoring(tracking) of nodes.

Step 2: Trusted

During this step, each node collects the data concerning the trust value of source to destination node. On the idea of trust value the distinction between legitimate and Sybil nodes are often created. If the trust value of the new node in routing table is greater and equal then that node as legitimate node and otherwise it's considered as Sybil node.

Step 3: Isolation

Into this assumption the speed of nodes is measured. This proposed method used isolate to multipath way for preventing Sybil attack. During this step, nodes must be enable or capable of adopting the changing in network. The changes are it may be path change for transmission or it may be an attacker.

3.2 Algorithm

Step 1: Start Hello packets 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 be change the path
    Else
        Legitimate node    // same path uses.
```

3.3 Flow Chart

The main steps used in the proposed method are shown in the flowchart. The flowchart shows the main steps used in the proposed method which are explained at later steps.

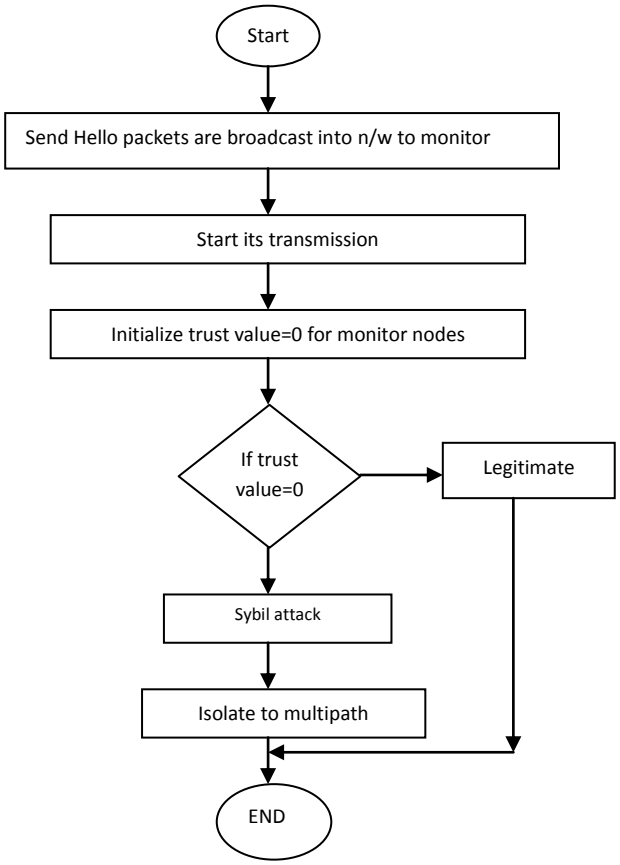

Fig.2: Flow Chart for Detection and Prevention of SYBIL Node

4. SIMULATION RESULTS

The simulation tool used for implementation is NS 2.35. In this we implemented the Sybil attack detection and prevention technique using DSR.

Parameters used for performance measurement are following:

1. Throughput: Total number of packets delivered over the total simulation time.

2. Packet Delivery Ratio (PDR): Ratio of data packets received by the destination to those generated by source

3. End to End Delay: It can be defined as the time a packet takes to travel from source to destination.

Table 1. Shows Simulation 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 address	802.11

For the performance analysis of routing protocol DSR, a regular well-behaved network is used as references. The experimental results are being elaborated under NS-2 Simulator. Also, our scenarios are tested in NAM for better understanding of the nodes movement and behavior (see figure).

Fig.3: Sybil attack detect and prevent

In above figure, Experiments are run on different number of nodes. The proposed method set trust value is equal to 0. When monitoring is started. After that we check trust value of all nodes. If trust value increases after transferring than node is legitimate node otherwise Sybil attack is detected.

In figure, when node colour is red then Sybil attack is detected and if node colour is blue than node is under observation.

4.1 Results Obtained

For this proposed work, following are three graphs showing the performance of proposed method results:

4.1.1 Average Throughput

The given graph demonstrates the relationship between the Throughput and varying mobility speed. In this graph there are three types of waveforms which are represented by red, green and blue colour. The red colour waveform represents proposed method, green colour waveform represents Existing Sybil Detection method and blue colour waveform represents DSR protocol's performance. In the graph this proposed method results are shown below by red colour waveform. It shows that performance of proposed method is improved to existing method for throughput.

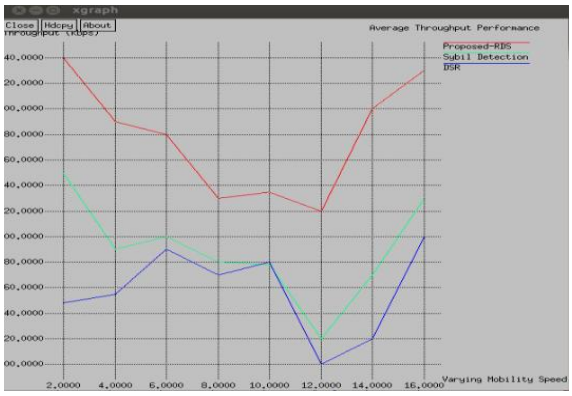

Fig.4: Performance of Average Throughput Analysis

4.1.2 Average End to End Delay

The given graph demonstrates the relationship between the End to end delay and varying mobility speed. In this graph there are three types of waveforms which are represented by red, green and blue colour. The red colour waveform represents proposed method, green colour waveform represents Existing Sybil Detection method and blue colour waveform represents DSR protocol's performance. In the graph this proposed method results are shown below by red colour waveform. It seems that end to end delay is greater in proposed method from existing system. This proposed method removes limitation of existing system.

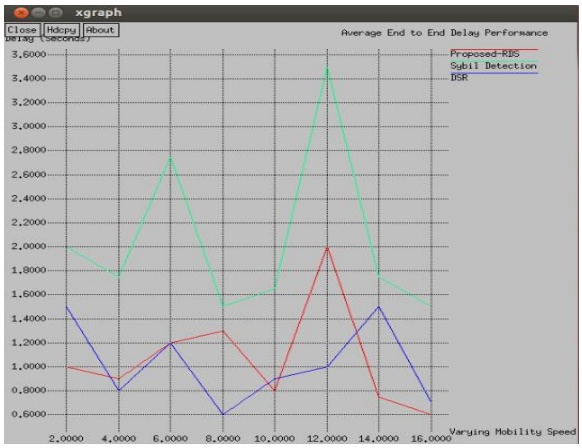

Fig.5 : Delay performance Analysis

4.1.3 Packet Delivery Ratio

The given graph demonstrates the relationship between the PDR and varying mobility speed. In this graph there are three types of waveforms which are represented by red, green and blue colour. The red colour waveform represents proposed method, green colour waveform represents Existing Sybil Detection method and blue colour waveform represents DSR protocol's performance. In the graph this proposed method results are shown below by red colour waveform. In the graph , comparison of PDR for different nodes. It is clear from graph that the performance of proposed system is superior over existing method.

Fig.6: Performance of PDR Analysis

5. CONCLUSION & FUTURE SCOPE

5.1 5.1 Conclusion

In this work, outlined trust based method for Sybil attack detection and prevention in MANET. We investigated this method using network simulator. The practical investigation of this method is done by considering three network conditions such as presence of Sybil attacker nodes in network, existing approach to detect such Sybil attackers in network and proposed approach to detect and prevent from such Sybil attackers in network. The performance comparison is done between these three kinds of network conditions with aim of achieving performance of proposed method is similar to existing network condition. From results it is clear with trust based with presence of Sybil attackers, the investigated method works efficiently and does not results into any data loss.

This method also removes limitation of existing method is that high end to end delay as compared to network condition.

5.2 Future Scope

From results it is clear with trust based method works efficiently and does not results into any data loss. The only limitation of this method is that used to extra trust node which is the future work for this research.

6. REFERENCES

[1] Mohsin Mulla and Santosh Sambare (2015) "Efficient Analysis of Lightweight Sybil Attack Detection Scheme in Mobile Ad hoc Networks" *IEEE systems journal International Conference on Pervasive Computing (ICPC).*

[2] J. R. Douceur (2002),"The Sybil Attack," presented at the Revised Papers from the first Int. Workshop on Peer-to-Peer Systems, pp.251-260,2002

[3] Anamika Pareek and Mayank Sharma (2015) "Detection and Prevention of Sybil Attack in MANET using MAC Address" *International Journal of Computer Applications(0975-8887),Volume 122- No.21, July 2015*

[4] M. Elboukhari, M. Azizi and A. Azizi (2015)," IMPACT ANALYSIS OF BLACK HOLE ATTACKS ON MOBILE AD HOC NETWORKS PERFORMANCE" *in International Journal of Grid Computing & Applications (IJGCA) June 2015, Vol.6, No.1/2.*

[5] Z. Kasiran and J. Mohamad (2014), "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.

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

[7] P. Chahal,G.K. Tak, and A.S. Tomar (2015) "Comparative Analysis of Various Attacks on MANET " *International Journal of Computer Applications (0975 – 8887), February 2015, Volume 111 – No 12.*

[8] R. Garg, H. Sharma (2014)," Comparison between Sybil Attack Detection Techniques: Lightweight and Robust" in *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2014, Vol. 3, Issue 2.*

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

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

[11] S. Upadhyay and B. K. Chaurasia(2011), "Impact of Wormhole Attacks on MANETs", *2011, vol. 2, Issue 1.*

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

[12] Z. Han, L. Lu, and M. J. Hussain (2014), "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)*, pp. 978–985.

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

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

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

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

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

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

[20] Y. Liu, D. R. Bild, R. P. Dick, Z. M. Mao, and D. S. Wallach(2015), "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.

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