Accusation Based on Non-Voting Mechanism in MANET using Clusters

Jayanthi. E, Mohammed Ali Hussain

***Abstract**: One of the challenges in MANET is authentication. To aid authentication, digital certificate are used by all the nodes in MANET. The network performs well if the nodes are trustworthy and cooperate properly. The certificate of the misbehaving nodes is revoked by certificate authority, there by debarring them from the network. The objective of this paper is to identify the malicious nodes which drop the packet deliberately to disrupt the network. Any node accusing the malicious node is inserted in the white list and the accused node is inserted in the blacklist based on Non-voting mechanism. The nodes placed in the black list are barred from the network. . Packet dropping due to link failure, mobility and traffic load intensity is excluded for accurate detection of the malicious node. Cluster based Non-voting mechanism with watchdog shows better performance in terms of better packet delay rate, packet delivery rate and packet loss rate while transmitting data. Clustering mechanism helps to reduce the communication overhead and certificate revocation provides secure network. Also, the false accusation is reduced as not all nodes accuse without proper analysis, with fear of being put on the whitelist, and being denied of further accusation. The algorithm is studied theoretically and evaluated practically using NS-2 to show better performance.*

Index Terms: blackhole attacks, network security, non-voting mechanism, and watchdog.

I. INTRODUCTION

In recent years a lot of scientists and researchers are working on wireless communication due to the current growing demand. MANETs are battery operated nodes with limited resource. Set up and configurations of MANETs are easy as the working principles do not rely on any fixed infrastructure. MANET is widely used in military area such a mountain terrain, snowy area etc., where setting up the infrastructure is difficult, the next to emergency rescue area where infrastructure is destroyed, and temporary network setup is required. MANETs are used in viable domains including information transfer among different people, conference and agreement representations. It is also used to set up Personal Area Network (PAN) for communication among several wireless devices like cellular phones, personal digital assistants and laptops. And recently it is used in MANET-VoVoN for call tracking using private signaling protocol.Owing to various applications MANET are preferred. Creating trustworthy security services for MANET is a challenging task. Following are the technical challenges of MANET. The communication process is very unpredictable over wireless medium with bit error as compared to the wired network. The requirement of prior information regarding the broadcast feature and protocols required for reliable communication for MANET. Device mobility and frequent topology change is another important challenge. Further, its limited Processing capabilities, memory storage, energy and bandwidth are the required for algorithm implementation in MANET. MANETS [2] are vulnerable to attacks than its counterpart wired network. Vulnerabilities actors in Ad hoc networks are Absence of integrated observing and management, limited battery backup, power supply, infrastructure-less network with limited resources, frequent disconnections and partitions due mobility. Due to the above vulnerabilities, MANETS have to accomplish security goals.

The major network security goals are confidentiality, and authentication. While compared to integrity, authorization availability and non-repudiation. In MANET, a number of communication approaches among nodes approaches are unicasting, multicasting, broadcasting, geo-casting and converge casting. These approaches are useful for successful communication in MANET. But, the characteristics and communication approaches of MANET present problems for achieving challenges and the security goals. Trust management is required to betterment the secrecy and security of MANET. The service of Watchdog is to monitor routing nature of a node, and then feed the information into the reputation system to manage and maintain the node reputation and thereby detection of black hole attack. The advantage of the watchdog is that it needs only local information for the detection of malicious node.

A. Passive and active attack

The attackers may delay the message/packets from reaching the destination, drop the packets or change the messages. The attacks are listed into two classification, viz. passive and active attacks. The passive attackers indulge in monitoring or eavesdropping of data, during the transmission of data in the network. The attackers do not attempt to tamper or modify the data in transit. Detection of passive attack is difficult, hence passive attacks need to be prevented rather than detecting and taking corrective actions. In other words, passive attacks do not indulge modifications to the original message contents. Passive attacks are further sub classified into two categories.

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

Jayanthi. E*, Department Computer science and Engineering, KL University, Guntur Dist., A.P., India

Dr.Mohammed Ali Hussain, Department Computer science and Engineering, KL University, Guntur Dist., A.P., India

First is release of message contents, where the sensitive information from the data are monitored during its transit. And the second type of attack is traffic analysis, here attackers may not get access to the data, but may know when and from where the message was transmitted from. This is used for predicting the nature of the information. Active attacks, on the other hand, involves

modification or tampering of messages on the transit. Prevention of active attacks is very difficult. Active attacks comprises of Denial of Service Attack (DOS), Replay attack, Masquerading, and alteration. The black hole is an example of an active attack. Where in the attacker drop the packets which are received. Two major types of attacks namely internal and external attacks are discussed in [4].

B. Cluster formation and Cluster head selection using trust based solution

Clustering is the process of dividing the network into groups, with respect to different requirements. The goal of clustering is to achieve good scalability for large networks, where nodes have high mobility. Nodes in the cluster have different roles to be played like cluster head is the coordinator of a cluster, while cluster members are regular node and the node with inter-cluster links which forwards information between clusters are cluster-gateway. Nodes in cluster perform route discovery and maintenance. There are two types of cluster routing– Flat routing works better for small networks, but is not efficient for large MANETs. Hierarchical routing is good for large networks. Clustering achieves communication scalability, optimize the coordination of network resources. Decreases retransmissions and collisions of packets, eventually balance resources in clusters. Also, Inter-cluster communication is between cluster-heads and cluster-gateways. Cluster heads make the local update and maintain cluster information. There are a different type of clustering based on route maintenance, mobility, energy availability, number of nodes per cluster and maintenance cost. [3] Authors illustrate the comparison between flat and cluster-based routings in MANETs with performance. Misbehaving nodes and cluster heads are burdened with the huge task which drains the available energy and reduces the total lifespan of MANET. Hence selection of worthy cluster heads is significant for better performance of the network. In [1], the author proposes an efficient trust model for choosing cluster head. Here trusted cluster head is elected to ensure secure communication through cooperative nodes. To reduce the overhead nodes are clustered based on the number of nodes. To compute trust of an individual node, nodes monitor the type of operations and behavior of neighboring nodes. And this information from its neighbors is used to decide the trust of the node using quantitative trust evaluation algorithm. Trust-based Low Energy Adaptive Clustering Hierarchy [5] uses monitoring module and trust evaluation module. TLEACH performs better than LEACH since about 50% of the data communicated by cluster members is accessed using gateway. Disadvantages of TLEACH is that it lacks monitoring of cluster head and does not control data loss. Li et al. [6] Manage trust in 2 parts, reputation-based framework and trust establishment framework. The former uses direct observation from one hop neighbor and indirect observation from other nodes. While the later part of framework investigates and assesses neighboring nodes with direct observations. Trust among neighboring nodes are accessed through opinions from all intermediate nodes in the MANET.

C. Routing protocol

Routing is research challenge in MANET. Routing algorithms goal in MANET is to perform routing with the constraints of changing topology, existing power available, low bandwidth, error rates and mobility. This sections shows a overview of how the routing protocols are classified in MANET. Routing protocols are classified as proactive and reactive protocols. Proactive routing protocols uses table driven approach. Huge overhead is incurred because of frequent route change. A better alternative is reactive approach where the routes are updated only on demand. Types of reactive routing protocols are DSR (Dynamic Source Routing), ABR (Associativity Based Routing), PAR (Power Aware Routing), LAR (Location-Aided Routing), TORA (Temporally-Ordered Routing Algorithm), CBR (Cluster Based Routing), AODV (ad hoc On-Demand Distance Vector Routing), SSR (Signal Stability Routing).

One of the most famous algorithm for routing is Adhoc on Demand Distance Vector (AODV) [7]. AODV is applicable in all most all the application where the mobile nodes keep moving, with the change in topology. There three packets used for controlling the flow of packets during routing, namely RREQ, RREP and RERR. RREQ is used by the source node to the neighboring node, to request the path to the destination. The nodes which know the route to the destination, reply to the source send RREP to the source node. With the help of RREP new path is created. RERR is used during routing, when a path is disconnected. In black hole attack, the attacker node claim to have route to reach the final node. The source node on receiving the RREP, sends the packets to malicious nodes. Now the malicious nodes drops these packet, thereby decreasing the performance of the network. Such malicious node need to be detected and removed from the network. When packet drop ratio of any node is less than threshold, then the node is the detected as black hole, and removed from the network. Our proposed methodology non-voting mechanism is used to detect the malicious node. In non-voting mechanism the accusing node and the accuser node both are punished, which is known as suicide for common good. This mechanism is used to increase the detection and removal of malicious node faster than the voting mechanism. Also reduces communication overhead.

D. Non-voting based mechanism

In this mechanism, a regular node with a certificate can blame a misbehaving node. According to J. Clulow et al proposal, the accused node can be quickly revoked from the network with just one accusation. But in this mechanism, the certificate is revoked from not only the accused node but also from the accuser. This approach is called suicide for the common good. The accusing node surrender/sacrifice itself to secure the network by getting rid of an attacker node from MANET. The advantages of non-voting mechanism is faster detection and removal of the node from the network and to reduce the overhead required for communication. This method is best suited for immediate barring of the node before any adverse attack occurs in the network.

Moreover, further filtration and differentiation of accused and non-accused node can be dealt with by using voting based mechanism.

II. LITERATUTE REVIEW

There are many ways to detect the nodes which drop packets. Our methodology provides efficient and quick detection of malicious nodes as compared to the following work proposed by authors.

In approach [8], Jaisankar et al. each node has Blackhole Identification Table. If the packet delivery ratio is more than the threshold, the node is declared as a misbehaving node and removed from the system. Chavda et al [9] detect black hole attack but incurs a huge communication overhead. [10] Presents a survey on major types of network layer attack and also discusses (Intrusion Detection System) IDS and (Intrusion Prevention system) IPS mechanism.

A lightweight algorithm [11] finds the black-hole nodes in the network using on-demand routing protocols and shows good outcome in terms of delivery packets and throughput.. The probability of packets received at the destination is calculated as Pd = Nd/Ns. Nd is the size of packets acknowledged and Ns is the size of packets directed. TT is the threshold. If Pd< TT, then the malicious device is detected in the path. If not, then it collects special ack from the endpoint. Detection algorithm start if the packet loss exceeds 20 percent of the total packets directed by the originator. In [12] author describes the network layer attacks and also various solutions and detection methods for attacks on black hole. Paper [13] summarizes the pros and cons of the existing routing protocol in MANET. Single and collaborative black hole attack are discussed in detail and in the tabular column in chronological order. Paper also discusses and concludes that a hybrid detection method. This method uses the benefits of reactive and proactive routing. Few key encryption methods with hashing methods are used to solve the problem due to routing mechanism. [14, 16] uses trusted AODV routing protocol, where trust of the nodes are calculated using the tangent hyperbolic function. Results show improvement in end to end delay, throughput, end to end delay and PDR (Packet Delivery Ratio) when compared to collaborative black hole AODV. Here [15] the proposed categorization classifies the detection approaches into two types based on the type of computation they perform, firstly computationally limited and secondly computationally intensive. Computationally intensive techniques are based on techniques such as Genetic Algorithms, Fuzzy Logic, Clustering Algorithms, and Mobile Agents for the discovery process. Whereas computationally limited techniques are based on the management of network parameters like trust between nodes, sequence numbers etc., for detection. The paper describes the taxonomy of algorithm in a very systematic way. [16, 17] here the effects of black hole and wormhole are mitigated using a trust. Trust value is computed with the type of response received with route request, route reply and data packets. Trust values are obtained between the values 0 and 1. If the trust values are less than 0.5 , then this misbehaving device is no longer retained in the network. The research paper [19] is classified into 3 scenarios for without attack, with the attack, and preventing the attack. The parameters used for performance are throughput and PDR for against a number of nodes, speed, and pause period and coverage space to detect black hole attack. Work shows network performance with an increase in mobile nodes. Also shows quick detection of the black hole. But the blackhole impact is degraded due to the increase in node speed. [18][20] Shows the properties of routing attacks. Adhoc on Demand Multipath Distance Vector) routing protocol is used to mitigate the black hole attack the work also shows reduced overhead. In [21] authors include a fine-grained analysis scheme for detecting malicious node using packet loss. This scheme does not uses clusters for malicious node detection, hence consumes more communication overhead. [22] Uses voting based mechanism to detect malicious node using frequency of votes and confidence weight of each node. But the disadvantage of voting based mechanism is false accusation. Hence our paper uses non-voting based mechanism to detect malicious node using clusters.

III. PROPOSED METHODOLOGY

This proposed system detects malicious node by analyzing packet dropping nodes using a watchdog mechanism. Watchdogs have the advantage of using only local information and hence are robust to most of the attacks. This method also uses clustering hence experiences reduced routing, reduced storage and overhead. This method also uses clustering hence experiences reduced routing, reduced storage and overhead. The cluster member are monitored and managed by the cluster head. All the cluster are in co-ordination with certificate authority. The certificate authority manages whitelist and blacklist as in [26]. The cluster member if detects any node misbehaving, then it reports to certificate authority to insert the node into the blacklist. The accuser in inserted in the whitelist. The nodes in the blacklist are barred from the network. And the nodes in the whitelist cannot accuse any other nodes. Fig. 1 shows node C as a malicious node, S and D as the source and destination nodes respectively. Initially, the source node S sends RREQ to all one-hop neighbors. B2 can be assumed to be the cluster head. Actually, after receiving RREQ packet from S, each neighbor node has to rebroadcast RREQ packet when routing table towards the destination is unreachable or RREP if the routing path is available. In Fig 1 the below node, C intrude upon the rule. Though it does not have a route to a destination it claims it has a route by replying with RREP to S. Since node C has replied positively about the route D, node S starts transmitting data packets via C. C starts dropping the packets and thereby degrades the performance of the network. Now when the neighboring nodes find or notice the misbehaving activity by C, informs the Certificate authority (CA). CA maintains the CRL [25], it inserts the accusing node in the warned list and the accused node in the blacklist. The nodes in the white list cannot accuse any other node. And the nodes in the blacklist is revoked and cannot participate in any network activity. Here we assume cluster heads do not drop packets. Any node even if it accuses cluster head, CA will not punish Cluster head either in the blacklist nor a warned list.

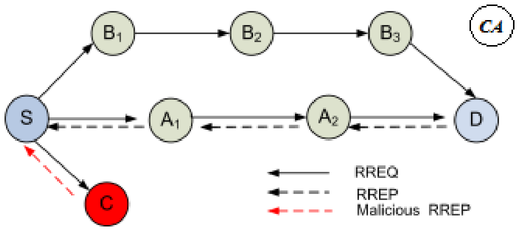

Fig 1: Malicious node detection in MANET using AODV

All the nodes are implemented with the watchdog mechanism, used to monitoring the behavior of the nodes in promiscuous mode. We implement the watchdog tool on top of AODV. The Watchdog mechanism is used to find out malicious nodes, which do not frontward packets and simply discard it. Watchdog is the basis of many malicious node detection algorithms. The watchdog mechanism monitors their downstream neighbors' locally to detect black hole node, by using overheard messages. If a watchdog detects and finds out for a certain time that a packet is not forwarded, it informs the certificate authority about the misbehavior. And secondly, if the node only receives the packet and does not forward, watchdog informs to the certificate authority about the malicious behavior. Also before sending the accusation, the nodes have to find out the through a various mechanism, the cause for packet dropping because of suicide for common good. Once the CA receives misbehaving activity, it inserts the accusing node in the white list and blamed node in the blacklist. Hence debar the accused node from dropping packets.To find out real misbehaving nodes, it is required to analyses the reason for packet loss. The working of the system may fail if innocent nodes are punished and the malicious nodes may continue unnoticed. Hence we try to find an approach that identifies the cause for packet losses with malicious RREP that leads to black hole attack. Our scheme identifies malicious nodes by calculating the actual packet drop by malicious node excluding the packet loss incurred due to link failure between two nodes, queue overflows or node mobility in MANETs [23, 24].

A. Link failure between two nodes

Good link between 2 nodes is used to gauge the efficiency of the channel and the malicious node. AODV is a reactive protocol it periodically broadcasts hello messages uses the Hello messages to inform its neighbors about the link to the host is alive. To ensure one hop count, The Hello messages are broadcasted with TTL equals to 1. As soon as the host receives the Hello message, there will be revision in the routing table. But if the host does not receive the information from the neighbor for say 'x' time, then the routing information is marked as deleted in the routing table. Once routing information is lost RRER message is generated to inform neighboring hosts about the link breakage and causing inefficiency. P_M is the formula for calculating the packet forwarding probability P_M at the MAC layer among the two nodes is as follows:

$$P_M = \frac{\xi_{recv(t_{i-1},t_i)}}{\xi_{exp(t_{i-1},t_i)}} \qquad (1)$$

During the interval (ti−1, ti), ξrecv and ξexp are calculated where total count in HELLO packets received ξrecv and the expected count in HELLO packets ξexp. And the probability of packet drop by the malicious node by not forwarding is

$$P_M = 1- \frac{\xi_{recv(t_{i-1},t_i)}}{\xi_{exp(t_{i-1},t_i)}} \qquad (2)$$

B. Traffic load Intensity

Some times when the rate routing traffic is very high, packets may not be totally transmitted or may be sent with low rate, leading to unproductivity. In MANET packets will be destroyed when the queue is filled due to queue overflow and multiple TCP flows back off. Also the delay due to packet drop by the queue and notification received by the sender, a large number of packets will be discarded. And also packets may be dropped due to congestion when the queue length increases. The average traffic load is formulated as below at node B.

$$TL_B=1/Q \sum_{j=1}^{N} q_j \qquad (3)$$

Where Q is the total number of queue samples gathered for a specified interval of time. Let q_j be the jth packet at the current time. $q_{max\ is}$ the max length the queue. Then at node B the traffic load intensity is calculated as follows.

$$TLI_B = TL_B/q_{max} \qquad (4)$$

Therefore if packet forwarding probability due to queue overflow and congestion is shown as

$$P_Q = 1- TLI_B \qquad (5)$$

Then the probability of forwarding probability due to alicious node dropping packets is given as

$$P_{Q\,=}\ \ TLI_B \qquad (6)$$

Here higher the value of TLI lesser is the probability of packet forwarding and smaller the value of TLI higher is the probability of packet forwarding by node B. hence it is evident the P is the probability of packet forwarding by malicious node by dropping other packets. Also, there are 2 more approaches to find the Dropping probability due to the malicious node. PQ_{t1} the actual forward probability at time t1 and PQ_{t2} is actual forward Probability at any random time. If PQ_{t1} - PQ_{t2} = 0 then the malicious node is broadcasting about false link failure most of the time. And secondly, if all the neighboring nodes claim of link failure then also it is false-claim by the malicious node.

C. Packet dropping rate due to mobility

In our scheme, we operate in promiscuous mode so that when i packet by node B is forwarded to next hop also overhears the transmission of the same packet to another node. Hence the nodes can compute the mobility of the next hop node, i.e. the neighboring node's rate of the link. The rate is further used for finding the reasons for packet loss. The rate of link changes at node B is formulated as:

$$\eta B = \lambda B+\mu B \qquad (7)$$

Where λ_{B} = link arrival rate and μ_{B} = link breakage rate of the device *B.* The maximum link arrival rate λ_{max} and u_{max} is maximum breakage rate. Hence the rate of link changes is calculated as given below.

$$\eta = \lambda B+\mu B / \lambda max+ umax \qquad (8)$$

Hence the successful packet forwarding probability due to mobility is given as

$$P_{\eta}=1-\eta \qquad (9)$$

And the successful packet forwarding probability due to malicious node dropping the packet is given as

$$P_{\eta}= \eta \qquad (10)$$

Hence it is obvious from the above relation that packet forwarding probability due to mobility parameter and that of malicious node activity is one. If the link change rate is more than the forwarding then packet drop probability is less and due to mobility. If link change is less than the forwarding then pack drop is more and possibly due to the misbehaving node. Also, P_{n} = 1-η is the probability of successful forwarding. If P_{η}>= 0.7(threshold) then it is misbehaving node else it is due to mobility.

D. Algorithm of packet forwarding strategy

By adding all the three discussed in the previous section, the packet dropping probabilities index from node A to node B is

$$PI_{(A-B)} = (\alpha PM+\beta PQ+\gamma PN)/ (\alpha+\beta+\gamma) \qquad (11)$$

Where $\alpha+\beta+\gamma=1$.

α, β, γ are the weights allotted to the parameters. These values will be used by the domain administrator to balance weights of the parameters according to the application and network used. PI is calculated by each node. And then the compared the estimated threshold to detect the malicious node

```
Procedure Main

Initialize the MANET, with NN nodes where
NN= 1, 2, 3, 4, 5........... in ideal condition.
Watchdog implemented in all the Cluster members.
Start Route Discovery by Source Node NNs
NNs directs RREQ Packets towards the Destination NNd
Pause for all Route Replies.
PDRdetection()
CRRDetection()
DroppingProbabiltyIndex()

Procedure Main ()
If (Node ==malicious and Node== inefficient and Node
==Misbehaving)
{
Set node as abnormal node
}
Else
{
Set node as normal node
}
End if
End procedure
```

```
Procedure PDRDetection
    For all neighbor nodes, a do
        Total sent packet = Total forwarded packets + Total packets dropped
        PacketDropRatio = TotalForwardedPacketByEachNode/TotalSentPacket
            Calculate Average PDR (Packet Delivery Ratio) Value for each Node
            Threshold Value (thα) =1/NN Σi=1NN PDRi
    End for

If (PDR>th_α) (α is the threshold)
set node as NON-Malicious node
endif
else
set node as Malicious-Node
end else
End procedure
```

```
Procedure CRRDetection
CRR = (RQ-RR)
If (CRR>95%) {Set node as efficient} endif
    Else if CRR<95 and CRR >=35{Set node as average
    node}    endif                Else {Set node as
    inefficient} endif
endProcedure
```

```
Procedure DroppingProbabiltyIndex
η = λ+μ
P_η= η
```

$$TLB = 1/Q \sum_{j=1}^{N} qj$$

```
TLIB=TLB/q_max
Pq = TLI_B
Pm = 1-∑ recv(ti-1,ti)/ ∑exp(ti-1,ti)
DPI_(A-B) = (P_m+P_q+P_η)/(α+β+γ)
if (DPI>thα) (thα is the threshold)   then
set as Norma Node endif
else Misbehaving Node end else
End procedure
Stop Communication
End Process
```

The performance of the network depends on the following matrices such as:

a. Packet Delay
b. Response Time
c. QoS of Service Provider
d. Packet Forwarding Misbehavior

The accusing node computes Packet Drop Ratio (PDR) and Throughput. If for a particular node PDR is very high and throughput is very low the node is said to be accused and misbehaving.

But the nodes are in wireless environment, packets may be dropped due to congestion, link failure, overload, mobility and media interference. The packet drop only due to malicious node is calculated and the malicious node is inserted in the black list. And then the accused node is inserted in the white list.

SIMULATION RESULTS

The simulation analysis of the research is implemented using Network Simulator version – 2 (NS2) using the two-ray ground, omnidirectional antennal model with IEEE 802.1e simulation environment. The black hole simulation is assimilated in the 100 node MANET environment and the performance metrics Throughput, Packet Delivery Ratio, False Positive Ratio and End to End Delay are measured.

The analysis is carried out by comparing the MANET nodes in three different environments. First the normal simulation without any attacks, then including attack and source anonymity and finally including attack and non-voting based analysis with watchdog mechanisms.

Throughput

From the simulation analysis, it is shown that the MANET has better throughput performance while using non-voting based analysis with watchdog mechanisms than source anonymity without watchdog mechanism. Simulation values with normal data transfer are shown for reference. The simulation graph for Throughput metric is shown in Figure 2.

Packet Delivery Ratio: The ratio of the number of the delivered data packet to the destination. Σ Number of packet receive / Σ Number of packet sent. From the simulation analysis, it is shown that the MANET has better packet delivery ratio while using non-voting based analysis with watchdog mechanisms than source anonymity without watchdog mechanism. Simulation values with normal data transfer are shown for reference. The higher the value of the packet delivered ratio implies the better performance of the proposed watchdog mechanism. The simulation graph for Packet Delivery Ratio metric is shown in Figure 3.

False Positive Rate: The ratio of the false alarm generated for the attack detection to the total number of attack detection is defined as false positive rate or false alarm rate. It is defined as the detection of attack with alarm when the attack is actually not happened. From the simulation analysis, it is shown that the MANET has minimum false positive rate while using non-voting based analysis with watchdog mechanisms than source anonymity without watchdog mechanism. The simulation graph for False Positive Rate metric is shown in Figure 4.

End to End Delay: The period occupied for a data packet to be transmitted from source to destination. From the simulation analysis, it is shown that the MANET has minimum End to End Delay while using non-voting based analysis with watchdog mechanisms than source anonymity without watchdog mechanism. Simulation values with normal data transfer are shown for reference. The simulation graph for End to End Delay metric is shown in Figure 5.

Warned nodes vs. Malicious nodes: The ratio of the number of nodes warned during the non-voting process to the number of malicious nodes in the network is simulated and shown in Figure 6. From the simulation analysis, it is shown that the MANET has maximum warned nodes identification while using non-voting based analysis with watchdog mechanisms than source anonymity without watchdog mechanism.

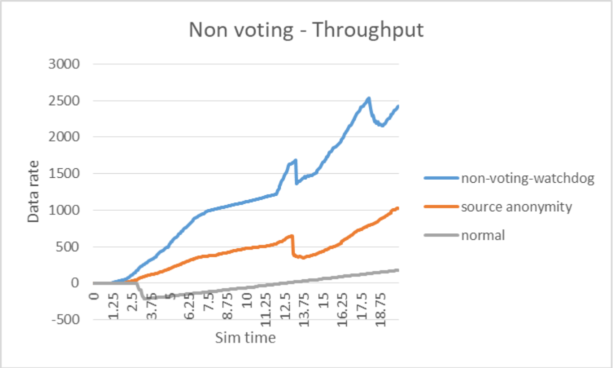

Figure 2: Simulation Graph – Throughput Analysis

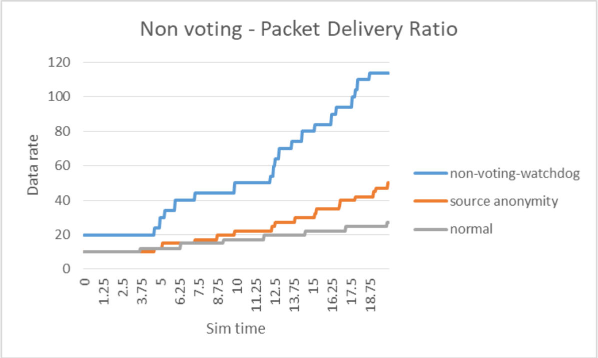

Figure 3: Simulation Graph – Packet Delivery Ratio Analysis

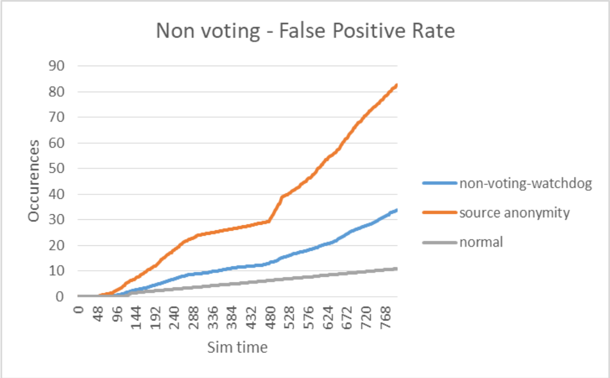

Figure 4: Simulation Graph – False Positive Rate Analysis

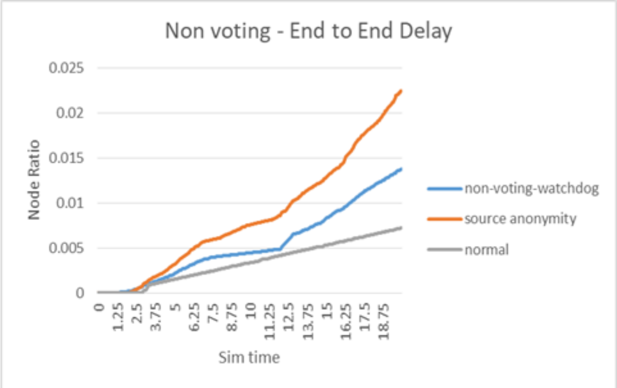

Figure 5: Simulation Graph – End to End Delay Analysis

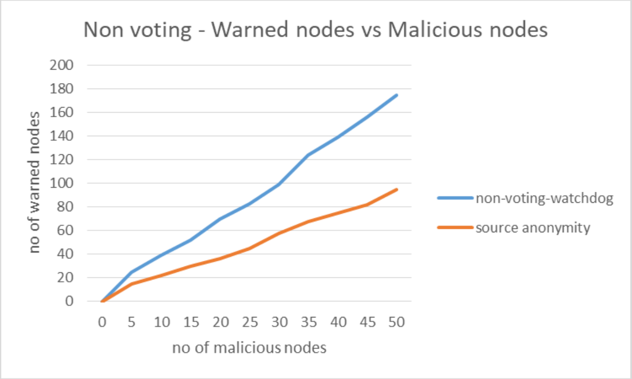

Figure 6: Simulation Graph – No of warned nodes vs. malicious nodes

IV. CONCLUSION

Watchdog-AODV increases the reliability of detection and provides secure communication for route discovery process without additional control packets. The proposed method shows that with slight modification to AODV with watchdog, clustering and non-voting mechanism helps to reduce the routing overhead. The causes for packet dropping like mobility, link breakage and traffic load intensity are excluded for the calculation of packet drop. Using the non-voting mechanism, the ratio of the warned nodes to the number of malicious nodes is increased considerably proving the concept of better detection analysis. Our work shows fast and good accuracy rate in finding the malicious node. The algorithm is studied theoretically and evaluated practically using NS-2 to show better performance.

REFERENCES

1. Ferdous, R., Muthukkumarasamy, V., & Sithirasenan, E. (2011). Trust-Based Cluster Head Selection Algorithm for Mobile Ad Hoc Networks. 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications.
2. Priyanka Goyal, Vinti Parmar, Rahul Rishi “MANET: Vulnerabilities, Challenges, Attacks, Application” IJCEM International Journal of Computational Engineering & Management, Vol.11, pp. 32-37, January 2011, ISSN: 2230-7893
3. Yu, J. Y., Xie, L. F., Zhang, M., & Chong, P. H. J. (2011). A Performance Comparison of Flat and Cluster Based Routings in Mobile Ad Hoc Networks. International Journal of Wireless Information Networks,
4. Tanupreet Singh, Jasmeen Kaur, "Trust based discovery and disposal of blackhole attack in mobile ad hoc networks", HCTL Open International Journal of Technology Innovations and Research, vol. 16, 2015Song, F., & Zhao, B. (2008). Trust-Based LEACH Protocol for Wireless Sensor Networks. 2008 Second International Conference on Future Generation Communication and Networking.
5. Li, R., Li, J., Liu, P., & Chen, H.-H. (2007). An Objective Trust Management Framework for Mobile Ad Hoc Networks. 2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring.
6. Arulkumaran, G., & Gnanamurthy, R. K. (2017). Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Adhoc Network. Mobile Networks and Applications.
7. Jaisankar N., Saravanan R., Swamy K.D. (2010) A Novel Security Approach for Detecting Black Hole Attack in MANET. In: Das V.V. et al. (eds) Information Processing and Management. BAIP 2010. Communications in Computer and Information Science, vol 70. Springer, Berlin, Heidelberg.
8. Chavda, K. S., & Nimavat, A. V. (2013). Removal of black hole attack in AODV routing protocol of MANET. 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT).
9. Nadeem, A., & Howarth, M. P. (2013). A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. IEEE Communications Surveys & Tutorials, 15(4), 2027–2045.
10. Saurabh, V. K., Sharma, R., Itare, R., & Singh, U. (2017). Cluster-based technique for detection and prevention of black-hole attack in MANETs. 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA). doi:10.1109/iceca.2017.8212712
11. Ranjan, R., Singh, N. K., & Singh, A. (2015). Security issues of black hole attacks in MANET. International Conference on Computing, Communication & Automation. doi:10.1109/ccaa.2015.7148419
12. Tseng, F.-H., Chou, L.-D., & Chao, H.-C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-Centric Computing and Information Sciences, 1(1), 4. doi:10.1186/2192-1962-1-4
13. Singh, S., Mishra, A., & Singh, U. (2016). Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm. 2016 Symposium on Colossal Data Analysis and Networking (CDAN).
14. Sherif, A., Elsabrouty, M., & Shoukry, A. (2013). A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET). 2013 IEEE 16th International Conference on Computational Science and Engineering.
15. Arya, N., Singh, U., & Singh, S. (2015). Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. 2015 International Conference on Computer, Communication and Control (IC4).
16. Singh, U., Samvatsar, M., Sharma, A., & Jain, A. K. (2016). Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol. 2016 Symposium on Colossal Data Analysis and Networking (CDAN).
17. Sathish M, Arumugam K, Pari, S. N., & Harikrishnan V S. (2016). Detection of single and collaborative black hole attack in MANET. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).
18. Nitnaware, D., & Thakur, A. (2016). Black hole attack detection and prevention strategy in DYMO for MANET. 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN). doi:10.1109/spin.2016.7566704
19. Rani, J., & Kumar, N. (2013). Improving AOMDV protocol for black hole detection in Mobile Ad hoc Network. 2013 International Conference on Control, Computing, Communication and Materials (ICCCCM).
20. Rashmi, Ameeta Seehra,”A Novel Approach for Preventing Black-Hole Attack in MANETs”, International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.3, September 2014 , pp 01-09
21. Khan, M. S., Midi, D., Khan, M. I., & Bertino, E. (2017). Fine-Grained Analysis of Packet Loss in MANETs. IEEE Access
22. MA Hussain., & S Naganjaneyulu . (2015). An Optimal Voting Mechanism for Cluster-Based Certificate Revocation in Mobile Ad Hoc Networks. Middle-East Journal of Scientific Research. DOI: 10.5829/idosi.mejsr.2015.23.09.22451.
23. Samar, P., & Wicker, S. B. (2004). On the behavior of communication links of a node in a multi-hop mobile environment. Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc ’04.doi:10.1145/989459.989478
24. J. Clulow and T. Moore, “Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems,” ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July 2006
25. Liu, W., Nishiyama, H., Ansari, N., Yang, J., & Kato, N., “Cluster-based certificate revocation with vindication capability for mobile ad hoc networks”, IEEE Transactions on parallel and distributed systems, vol. 24, no. 2, pp. 239-249, 2013.
26. Jayanthi. E, Mohammed Ali Hussain, “A Novel Approach Certificate Revocation in MANET using Fuzzy logic”.

AUTHORS PROFILE

Jayanthi.E M.Tech (NIE, Mysore). Her interest includes Compute Networks, MANET, Network Security. She has published technical papers both in National and International Journals in the area of Network Security, WSN and MANET. She has funded project from BCUD, Pune. She is a professional member of IAENG.

Dr. Md Ali Hussain, M.Tech.,Ph.D. His research interest includes Computer N/Ws, Wireless & Mobile N/Ws and Web Commerce. He published many number of technical papers both in National & International Conferences and Journals. At present he is serving as Program Committee Member of various International Conferences. He is Chief Technical Advisory Board Member, Chief Editor, Editor and Technical Reviewer of many International Journals. Received Best Academic Researcher Award 2012 from ASDF Research Group, supported by Pondicherry Government. He is a professional member of IACSIT, IRACST, IAEST, CST, UACEE, ISTE, IAENG, AIRCC, AICIT AND IARCS.