© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method

Neelam Janak Kumar Patel*[1], Dr. Khushboo Tripathi[2]
[1]Ph.D. Research Scholar, Department of CSE, ASET, Amity University, Haryana, India
[2]Assistant Professor, Department of CSE, ASET, Amity University, Haryana, India

ABSTRACT

A Mobile ad hoc network (MANET) is infrastructure less network and has numbers of mobile nodes. Any node can work as a router that receives and sends packets and routes them. Networks are highly affected by various types of attacks so securities are a challenges factor. Proper energy utilization becomes a challenging issue because of its highly decentralized infrastructure, dynamic topology and resource constrained. In this research paper, we use 32 mobiles nodes in the network, there are not any centralize control in the network so we implemented clustering technology for proper energy utilization of nodes. Dividing all nodes into three clusters, in each cluster selected cluster head which has maximum energy level. In MANET packet dropped or delayed by the malicious node. Hence, there is the need for effective intrusion detection system which can detect a maximum number of the intruder and corresponding packets be forwarded through some alternate paths in the network. We propose an alternate solution to detect the malicious node with help of trust value. It would remove the need for inbuilt IDS in the wireless networks and result in improving the performance of the network.

Keywords: Routing Protocols, Wireless Ad Hoc Network, MANET, AODV, Black hole, Gray hole

I. INTRODUCTION

MANET consists of numbers of self-directed wireless mobile nodes. Each mobile node works like a router which can route the data packets through neighboring node from source to destination in the network. They are self-controlled, self-organized and self-configured, and infrastructure-less networks [1]. MANET is extremely much susceptible to various types of attacks because of the use of wireless communication, dynamic topology, limited energy, and computing resources. There is not any centralized management for controlling the whole network, so in this paper, we can use clustering method. In hierarchical routing, architectures use the clustering is the universal technique. Means of hierarchical routing, the nodes of self-organized networks are distributed into a number of overlapping or disjoint clusters. One node which has maximum energy is selected as a cluster head for each cluster. This cluster head maintains the membership information for the cluster [3].

Classification of Routing Protocols:

Routing protocols can be classified into proactive routing, reactive routing, and hybrid routing in the MANETs [2].

Proactive or Table-driven Routing Protocol: A proactive routing is called a “table-driven” routing protocol [3]. This routing protocol maintains up-to-

date routing information and continuously evaluates routes to all reachable nodes. Using proactive routing algorithms, mobile nodes proactively update the network state and maintain a route regardless of whether data traffic exists or not, and the overhead to maintain up-to-date network topology information is high. Examples are –

- ✓ Destination-Sequenced Distance Vector (DSDV)
- ✓ Optimized Link State Routing (OLSR) Protocol
- ✓ Wireless Routing Protocol (WRP)
- ✓ Topology Broadcast Reverse Forwarding (TBRF)
- ✓ Fisheye State Routing (FSR)

Reactive or On-Demand Routing Protocol: Reactive routing protocols for mobile ad hoc networks are also called "on-demand" routing protocols [3]. In a reactive routing protocol, routing paths are established only when needed. Reactive routing protocol has minor setup delay for connections and recognition of the latest route to the destination; it does not situate any additional overheads on the network. It is loop-free, self-starting, and scales to a huge number of mobile nodes.

Examples are –

- ✓ Dynamic Source Routing (DSR) Protocol
- ✓ Ad hoc On-Demand Distance Vector (AODV)
- ✓ Cluster-Based Routing Protocol (CBRP)
- ✓ Temporally Ordered Routing Algorithm (TORA)

Ad hoc On-Demand Distance Vector (AODV) [4] protocol is the reactive routing protocol for MANET. In mobile ad hoc network, all mobile nodes are found a route from source to destination with the help of AODV. Data packets are transmitted only after the route is accepted. In AODV protocol that is three control messages that are Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). AODV route discovery process begins with the creation of a route request (RREQ) packet [5]. When a node wishes to send a packet to some destination, the source node broadcast RREQ packet to the network. It checks its routing table if it has a current route to the destination then forwards the packet to next hop node. If it has not the current route to the destination then it initiates a route discovery process. When a node receiving RREQ, it has a path to the destination then it creates RREP packet in unicasts. On receipt of RREQ message, after receipt of RREP every node increases hop count by one, intermediate nodes update their route entry with the new data in their routing tables.

Hybrid Routing Protocol: The combination of both proactive and reactive routing protocols are called hybrid routing protocols. Normally, the hybrid routing protocols for mobile ad hoc networks utilize hierarchical network architectures [1].

Examples are –

- ✓ Zone Routing Protocol (ZRP)
- ✓ Distributed Dynamic Routing (DDR) Protocol
- ✓ Zone-Based Hierarchical Link State (ZHLS)
- ✓ Distributed Spanning Trees Based Routing Protocol (DST)

Attacks in MANET:

Attacks in MANET can be classified on the basis of its source, behavior, and nodes. On the basis of source, there are two types of attacks that are external attacks and internal attacks. On the basis of behaviors which are passive attacks and active attacks. On the basis of nodes that is collaborative attacks. According to Layer attacks on MANETs, there are so many active attacks on network layer which are called routing attacks for example Wormhole, Black Hole, Gray Hole, Flooding attacks etc [2]. Wireless ad-hoc networks engross no infrastructure; they are vulnerable to a various type of attacks. One of these routing attacks is Black Hole attack [3], also known as Packet Drop Attack. In Packet Drop Attack, using a compromising node attacker attract all the network traffic toward them. It cannot forward incoming data packets to destination nodes; attacker drops all the data packets or selectively transfers the packet to next node. A malicious node exploits this vulnerability of the route detection packets of the on-demand routing protocols, for example, AODV. In route finding the progression

of AODV protocol, intermediary nodes are responsible to find a new path to the destination.

II. RELATED WORK

K. Rama Abirami and M. G. Sumithra [1]. proposed two algorithms which are credit-based protocols namely Neighbor credit value based routing called AODV (NCV-AODV) and improved Neighbor credit value based Ad Hoc on demand distance vector (AODV) routing called AODV (iNCV-AODV) routing protocol for detection mechanisms against the selfish behavior attack. Uzma Shaikh and Arokia Paul Rajan [2].Proposed a secure and efficient methodology for the reorganization and avoidance of malicious attacks in MANETs. The proposed algorithm is done using IDS, these IDS keep watch on each and every node. If a malicious node finds it broadcast message to the whole network of nodes and maintain a routing table. Shashi Gurung and Siddhartha Chauhan [3]. Proposed a protocol for Justifying Black Hole effects through Detection and Prevention based on a dynamic threshold value of the destination sequence number (MBDP-AODV). This protocol performs better result as compared with existing one under black hole attack. VidyaKumari Saurabh, Prof. Roopesh Sharma et at. [4]. Propose d lightweight procedure is based on simple affirmation scheme to detect the black hole attack in MANET. That provided better results relative to Modified AODV approach. Deepak Kumar Verma, Renu Jain et al. [5]. Proposed IDS based on collecting the RREP messages from intermediated nodes and the destination. Using K-means clustering algorithm messages are clustering and identify the malicious node. Harmeet Singh and Dr. Jatinder Singh [6]. Proposed a new hybrid and secure clustering technique for detection and isolating black hole attack in MANET. Detecting the black hole attack using threshold values and provides a secure path from source to destination using clustering approach. Snehal P. Dongareand Prof. R. S. Mangrulkar [7]. Proposed a methodology for improving the lifetime of the wireless network using cluster head selection based energy-efficient protocols. Using this protocol efficiently minimizes the possibility of the negotiated node to turn into the cluster head and considerably improves network performance using parameters like Packet Delivery Ratio (PDR), Throughput and energy utilization in a wireless sensor network.

III. SECURITY LIMITATION IN MANET

In MANETs, it does not have any centralized control to transferring data packets from source to destination. Fig 1 (a). Shows that the numbers of mobiles nodes communicated with each other using clustering method. Three clusters are communicated with each other using cluster head, clusters heads are elected by highest trust values [7]. MANETs are vulnerable various kinds of attacks. A Black hole (False report) attack or Gray hole (Packet drop) attack is a type of denial-of-service attack proficient by dropping packets. Attacks on routing layer can be classified into two types, active and passive. In the passive attack, an attacker only eavesdrops the network activity it can not disrupt the operation of the network and can not affect the performance of the network.For example, Eavesdropping, traffic analysis, monitoring etc. In the active attack, an attacker can alter the original information of the data packets and disrupt whole network activity. For example, black hole, wormhole, gray hole, and sinkhole attack. In this attack compromise node is advertising the shortest and most efficient route and attract all the network traffic toward it. It can alter the information of the data packets and route wrong data to the whole network [6].

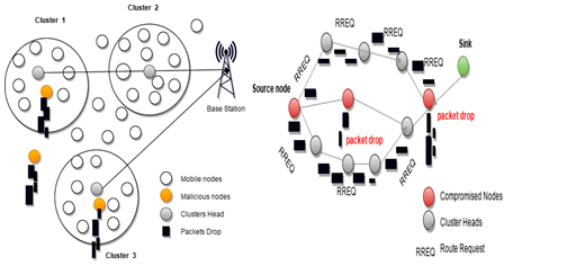

Figure 1.(a) Overview of Attacks in MANETs **Figure 1.(b)** Malicious node detection Model

Figure 1. Security Limitation in MANETs.

IV. PROPOSED ALGORITHM

If the number of packet drops nodes increases then the data thrashing would also likely to increase. A malicious node can initiate the following two attacks:

PACKET DROPPING: Source node broadcasting the RREQ to all nodes in the network and send the data packets. A malicious node cannot forward all the packets to its neighbor nodes, it drops all or a few of the packets that are supposed to be forward. It works like black hole attack or selectively forwarded attack.

PACKET MODIFICATION: A malicious node alters the entire information of the data packets and forwards it to further process. A malicious node randomly chose based on the number of packets dropped. So, sometimes genuine node also treated as the intruders or attacker. It works like a Spoofing attack in the network. At the end of the result into the high false positive rate and it violates the security of wireless networks.

PROPOSED TRUST VALUE BASED ALGORITHM: Figure 2. Shows the proposed algorithm is based on the trust values of individual nodes. Dividing all nodes into three clusters, in each cluster selected cluster head which has maximum energy level. Using energy level of the node we find trust value of each node in the MANET. After finding trust value we compare it with a predefined threshold value [4] and detect the malicious node after detecting we prevent it with consistent packets is forwarded through some alternate paths in the network.

In Figure 2 the algorithm includes the following steps.

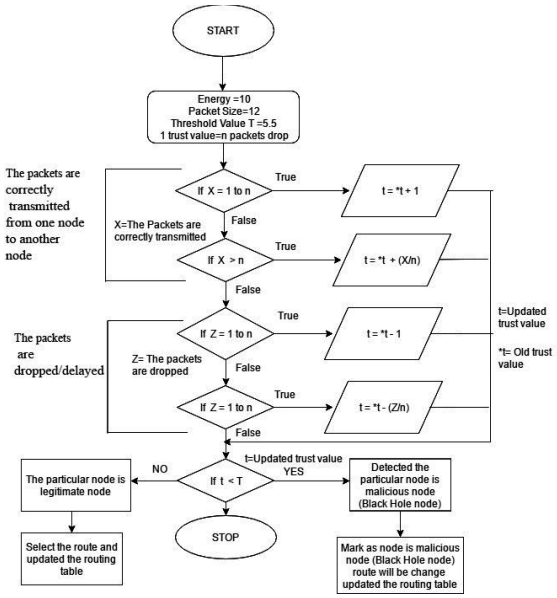

Figure 2. Proposed Trust Value based Algorithm

STEP-1 Initialization:

- ✓ energy is 10
- ✓ Packet size is 12.
- ✓ Nodes are dividing into three clusters. There are numbers of member nodes in each cluster. Using energy and bandwidth node we find trust values of all the participating nodes.
- ✓ Initialize the threshold value of the trust value with 5.5.
- ✓ 1 trust value = n packets dropped. (Assumption).

STEP-2 The trust value upgraded:

When the packets are properly transmitted from one node to another node find the upgraded trust values t:

- The trust values of the specific nodes incremented by one if the packets are between 1 to n.

Upgraded trust value t = old trust value *t + 1;

- If the packets are greater than n, then the upgraded trust value will be:

Upgraded trust value t = old trust value *t + (X / n);

When the packets are dropped or delayed find the upgraded trust values t :

- The trust values of the specific nodes decremented by one if the number of dropped or delayed packets is between 1 to n.
  Upgraded trust value t = preceding trust value *t – 1;
- The number of dropped packets is greater than n, then trust value of that specific node will be,

Upgraded trust value = preceding trust value *t – (Z / n);

The particular node has negative trust value, then print “Illegal node”.

STEP-3 Eliminating the malicious node from the network:

- If (t < T) upgraded trust value is less then threshold value.
  - ✓ Then the node is marked as a malicious node (Black hole node)
- If (t >T) upgraded trust value is greater than the threshold value.
  - ✓ Then the node is considered as a genuine node.
- Stop comparing the trust values of nodes with a threshold value.

V. RESULT AND ANALYSIS

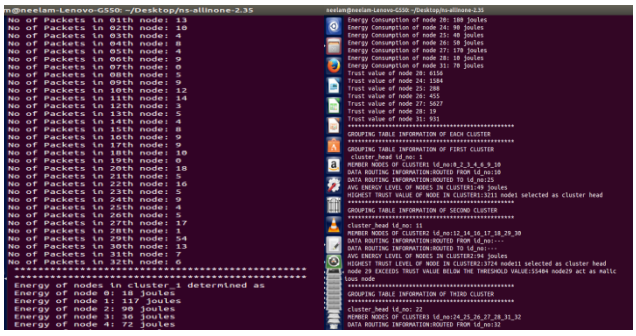

Figure 3. tcl file scenario execution.

Figure 3 shows the scenario execution of the .tcl file. In this figure we show that there are 32 nodes are communicated with each other using clustering technology. Here we use three clusters each and every cluster has elected cluster head by calculating the trust value of the node, highest trust value of the node is selected as a cluster head. We also show that the value of energy node and a number of the packet in each node.

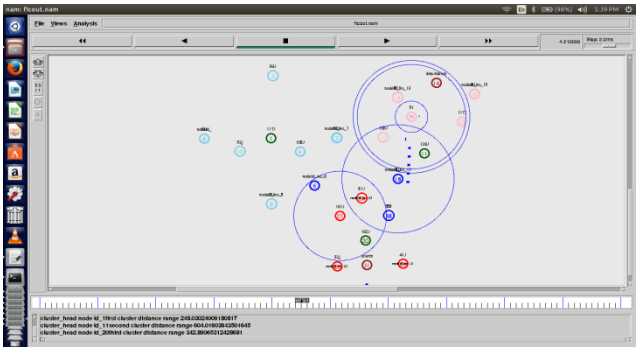

Figure 4. nam file for clusters packets route.

Figure 4 is the network animation for three cluster's member's nodes are sending and receiving the data packet from source to destination node. When finding the malicious node data packets are dropped. Using IDS we find the malicious node data packets are transferred through another route using this IDS algorithm we prevent the network from the malicious node.

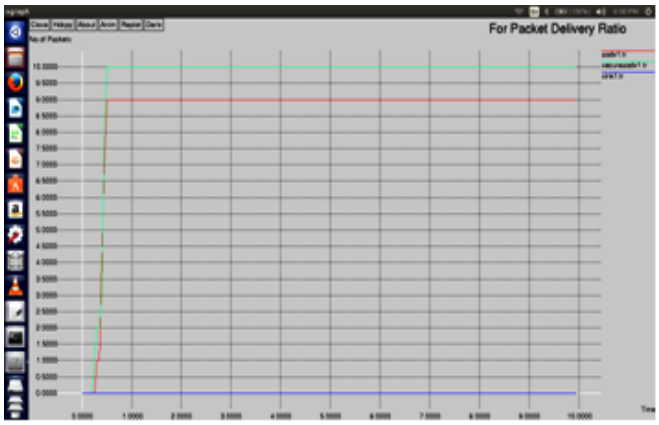

Figure 5. For Packet Delivery

Figure 5 shows the graph for packet delivery ratio for the without applying any routing protocol sink, applying Normal AODV routing protocol and implementing secure AODV routing protocol. We have seen that normally transferring packet to sink without applying any routing protocol that is 0 packets are delivering. After applying the Normal AODV routing protocol the no of packets is increased at the same time and packer deliver ration is increased.

At the same time, we applied our proposed secure AODV routing protocol has maximum no of packet transfer that increases the packet deliver ration compare to AODV.

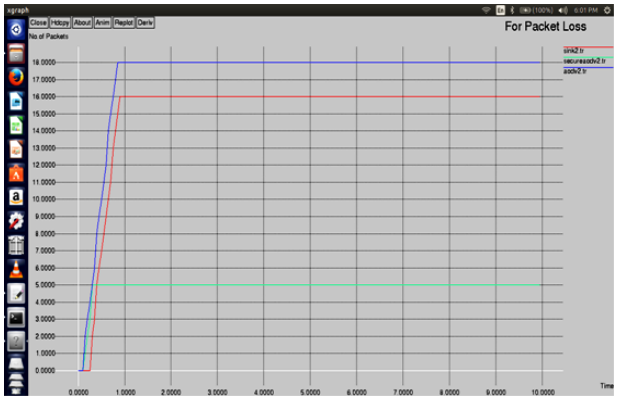

Figure 6. For Packet Loss

Figure 6 shows that the graph for packet loss. It analyses that the at the normal situation means without applying any routing protocol packet loss is 16 bit/sec at the same time applied AODV routing protocol we can see that the packet loss in increase up to 18bit/sec because implemented malicious node that dropped the data packet.In the same situation, we are applying our secure AODV routing protocol we can see the packet loss is decreased 5bit/sec. So we analyze that our secure AODV routing protocol is very effective to eliminate the malicious node from the route compares to Normal AODV.

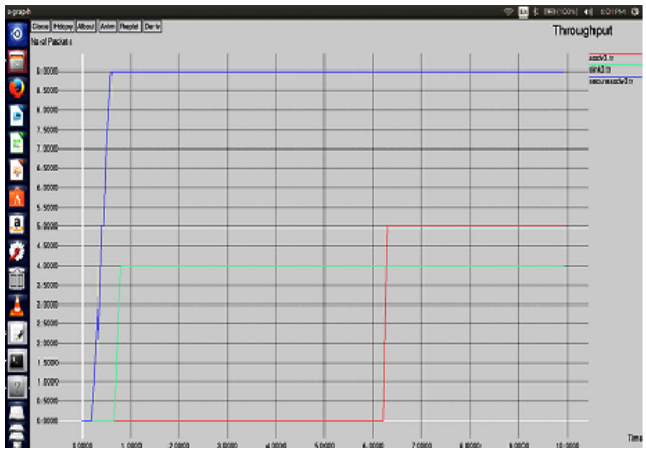

Figure 7. Throughput

Figure 7 shows the graph of throughput. It shows that the throughput of the secure AODV is higher than the normal sink and normal AODV.

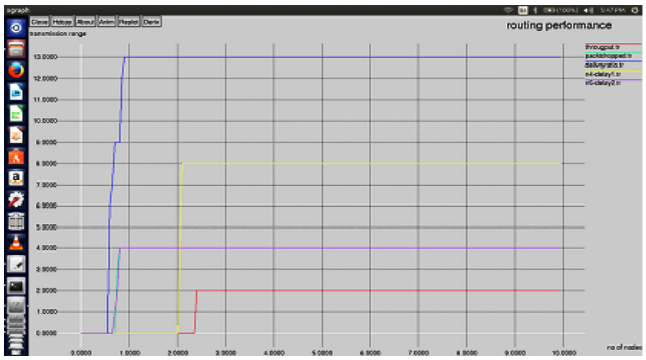

Figure 8. Routing performance

Figure 8 shows that the overall performance of the network with the different parameters likes throughput, packet dropped, delivery ratio and delay. When the no of nodes is communicating with each other according to the simulating time the packet delivery ration increases, so it analyses that the overall routing performance is increased.

VI. CONCLUSIONS

In our research work, we proposed a trust value algorithm using IDS AODV that secure the network routing activity from the attacker. MANETs does not have any centralized control so, we used clustering pattern analysis techniques, using clustering we find trust values of all nodes. We select the node as a cluster head which has maximum trust value. If the particular node is properly transmitted data packets from one node to another node, then each time the trust value of reliable node will increase by 1.When a trust value of a specific node is equal or more than the threshold value then it node will be considered as a genuine node for further communication. When a trust value of the specified node is less than the threshold value then it will be treated as the packet dropper or modifier node and it will be called as a malicious node for more communication. After detecting the malicious node in the network route data packets will be transferred from another path,

using this type of IDS we secure the network routing activity from attackers.

VII. REFERENCES

[1]. K. Rama Abirami, M. G. Sumithra, "Evaluation of Neighbor Credit Value Based AODV Routing Algorithms for Selfish Node Behavior Detection", Springer Science and Business Media Cluster Computing, Vol. 1https://doi.org/10.1007/s10586-018-1851-6,2018.

[2]. Uzma Shaikh, Arokia Paul Rajan, "Intrusion Detection and Avoidance of Black and Grey Hole Attacks using AODV Protocol Based MANET", International Journal of Engineering & Technology, Vol.7, pp.123-141, 2018.

[3]. VidyaKumari Saurabh, PROF. Roopesh Sharma, RavikantItare, "Cluster-based Technique for Detection and Prevention of Black-Hole Attack in MANETS", IEEE International Conference on Electronics, Communication, and Aerospace Technology ICECA, pp.489-494, 2017.

[4]. Shashi Gurung, Siddhartha Chauhan, "A Dynamic Threshold Based Approach for Mitigating Black-Hole Attack in MANET", Springer Wireless Network, pp.1-16, https://doi.org 10.1007/s11276-017-1514-1, 2017.

[5]. Deepak Kumar Verma, Renu Jain, Ashwani Kush, "Intrusion Detection using RREP Messages of AODV Routing Protocol", International Journal of Applied Engineering Research, Vol.12, Issue.9, pp.1956-1961, 2017.ISSN 0973-4562.

[6]. Snehal P. Dongare, Prof. R. S. Mangrulkar, "Optimal Cluster Head Selection Based Energy Efficient Technique for Defending against Gray Hole and Black Hole Attacks in Wireless Sensor Networks", Elsevier Procedia Computer Science, Vol.78, pp. 423-430, 2016.

[7]. Amol R. Dhakne, Prashant N. Chatur, "TCNPR: Trust Calculation based on Nodes Properties and Recommendations for Intrusion Detection in Wireless Sensor Network", IJCSNS International Journal of Computer Science and Network Security, Vol.16, Issue.12, pp.1-10, 2016.

[8]. Shikha Sharma, Manish Mahajan, "Security Mechanisms for Mitigating Multiple Black hole Attack in MANETs", IJISE International Journal of Innovative Science, Engineering & Technology, Vol. 2, Issue 11, pp. 582-588, 2015.ISSN 2348-7968.

[9]. Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, "BHIDS: A new, Cluster-Based Algorithm for Black Hole IDS", Wiley Inter-Science, Security and Communication Networks, Vol.3, pp.278–288, 2014.

[10]. Rajendra Aaseri, Pankaj Choudhary, Nirmal Roberts, "Trust Value Algorithm: A Secure Approach against Packet Drop Attack in Wireless Ad-Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.5, Issue.3, pp.99-111, 2013.

[11]. Fidel Thachil, K CShet, "A Trust-Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET", IEEE International Conference on Computing Sciences, ICCS, pp.281-285. 2012.

[12]. Ming-Yang Su, "Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems", Elsevier Computer Communications, Vol 34, Issue 1, pp.107-117, 2011.