Pak. J. Biotechnol. Vol. 13 special issue II (International Conference on Engineering and Technology Systems (ICET'16) Pp. 40 - 45 (2016)

SECURED MOBILE AD-HOC NETWORK WITH MODIFIED DSR AND SNUPM ALGORITHM

J. Gautam, K. Vishali and P. Malathi

Department of Information Technology, Velammal College of Engineering & Technology, Maduri, India
E.mails: gip@vcet.ac.in, vishalikannanit@gmail.com, malathipriyadharan@gmail.com

ABSTRACT

Security is a decisive requisite in Mobile Ad-Hoc Network (MANETs) when assessed to wired networks. MANETs are more suspicious to security attacks due to the need of a reliable centralized cloud and scanty resources. In MANET, we have malicious nodes that overcome the network protocols thereby diminishing the network's performance. The development of mobile networks has implicated the need of new IDS models to deal with new security issues in these communication environments. In this paper, we proposed a Secured Network using Promiscuous Mode (SNuMP) which is a part of Intrusion Detection System where it can repair the malicious nodes and convert back them into a normal node for effective network performance.

Index Term - MANET, Malicious node, Promiscuous mode, MDSR, SNuMP.

I. INTRODUCTION

The precept capacity of a network to exchange data among the user that are appended to the network. Wireless communication is almost used in homes to avoid the process of introducing cables with the wireless network is shown in Fig 1.

Fig 1. Wireless Network Communication

The one of the vital factor in network is Mobile Ad-hoc NETwork (MANET). A MANET is a type of ad hoc network that could alternate locations and configure itself on the fly. A MANET is generally defined as a network that has many unfastened or self sustaining nodes, more commonly composed of cellular gadgets or different mobile portions, that may arrange themselves in quite a lot of ways and operate without infrastructure or centralized administrator [1]. MANETs in general are used for communication in event of natural disasters, on business conferences, and battle field, illustrates the importance of guaranteed safety of data transfer between two nodes [2]. In a MANET, a malicious node directs fake routing data, putting forward that it has an superb route and causes other good node to route knowledge packets by way of the malicious one. Most secure routing protocols are designed to prevent hazards to security properties, such as: (1) Personality verification and non-repudiation; (2) resource availability; (3) plenitude; and (4) covertness and privacy by way of forging a routing message, a malicious node is intended to scramble the path, and then, further eavesdrop or drop the packets, posing a possible chance to protection properties (2, 3 and 4). An
intrusion Detection System (IDS) passively screens network visitors at more than one locations within your network with the aid of using IDS sensors.

II. RELATED WORKS

Yi-an Huang and Wenke Lee [1] approach is proposed to detect and isolate the misbehaving nodes. In this approach cluster-based detection method is used to address the run-time resource constraint problem.

Bounpadith kannhavong et al., [12] Proposed a method in which a survey of routing attacks in mobile ad hoc networks to define the current state of the routing attack and countermeasures.

Nan Kangetal [13] proposed a new ID called Eckanced Adaptive Acknowledgement (EAACK) that solves four significant problems of Watchdog mechanism, which are ambiguous collisions, receiver collisions.

Komninos, et al., [14] explored the authentication and intrusion detection challenges and proposed a detection mechanism for unauthorized and compromised nodes.

Nidal Nasser and Yunfeng Chen [15] proposed a approach based on intrusion detection system Ex-watchdog, which is based on one proposed solution Watchdog. Ex-watchdog solves a fatal problem of Watchdog.

Gurnam Singh [3] progress provides superior performance of throughput, packet Drop ratio and condensed packet loss when compared with older methods.

Nan Kang and Tarek [16] approach proposed for EAACK—A Secure Intrusion- Detection System for MANETs. This approach uses novel IDS named EAACK protocol for MANETs.

Tamilselvan and Sankaranarayanan [17] approach is proposed to detect, a node forwarding a packet checks if the next hop also forwards it.

III. OVERVIEW OF DSR

DSR (Dynamic source routing protocol) has pooled residences of both AODV and DSDV. It's an on-demand routing protocol. DSR doesn't uses periodic routing protocol [4]. The supply knows the entire hop-by-hop route to the destination [5]. These routers are stored in a route cache is shown in Fig 2. DSR is like AODV except every intermediate node broadcast a route request [6]. This route request incorporates destination deal with, supply handle and unique identification number.

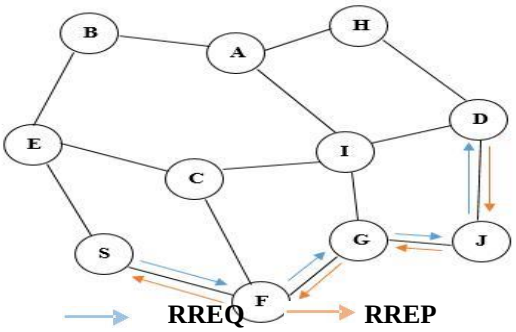

Fig 2. Determines shortest path using Dynamic Source Routing

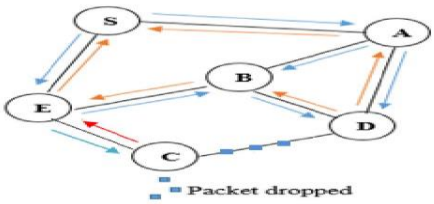

Fig 3. Packet Drop by Malicious Node

A. Route Discovery

In MANET, if a node is in need of sending data packets to a destination, initially it checks whether it has a pre-existing route for that destination. If so then it starts sending the data packets by that route. But if it could not find any pre-existing route, it initiates route discovery process with Route Request (RREQ) packets and simple floating technique is used[4]. Every node receiving this request rebroadcasts until it reaches the exact destination or the route to destination [5].

B. Route Maintenance

The mechanism where the sender detects if network topology has changed, then it no longer uses its route from source to destination. If any link is failed in source route, Route error (RERR) packet identifies the source node[4]. So that source node can use any other known route to the destination. Else the route discovery is done to find new route to destination. No expiration of routers-Using old route causes loss of data packets and network bandwidth.

a) Data salvaging - If an intermediate node encounters a failed or broken link, it can use an alternate route from its own cache[5].

b) Gratuitous replies - If the packet be routed with another node, sends a gratuitous reply to the source of route with better route [5].

IV. PROMISCUOUS MODE

Promiscuous mode is a type of computer networking operational mode where all network data packets can be accessed and viewed via all network adapters operating in this mode. It is a mode for a wireless network interface controller (WNIC) that causes the controller to pass all the traffic it receives to the Central Processing Unit (CPU) rather than passing only the frames that the controller is meant to obtain. This mode is generally used for packet sniffing that takes place on a router or on a computer related to a hub (instead of switch) or one being part of a WLAN. Promiscuous mode is often used to diagnose network connectivity issues. Promiscuous mode permits a network device to intercept and read each network packet that arrives in its entirety. First, it enables collection of local information without any additional communication overhead.

Fig 4. Creating 100 nodes

Second, the process of local traffic observations without disturbing the other node is made less complicated. Promiscuous mode mechanism deals the new method which has two parts: By using the Performance analysis part which gives the probability of packet received by the sender or the next hop i.e., packet drop. The next mechanism is Quick local repair scheme which makes use of nodes working in the adaptive Promiscuous mode when the expected constrains of the nodes drops down beyond a specified value.

In Fig 3., the node C (malicious node) gets the information from the destination in the form of packets, drop the packets and send fake information to the source. So that, it is referred as malicious node.

V. PROPOSED METHODOLOGY *A.*

Network Formation

Simulation is regulated making use of NS2 2.35. Because of the link stability and route lifetime, no route overhead was ruminated in our simulation. In 500X500 area mobile nodes exist. Square area is used to expand average hop length of a route with relatively small nodes. Each mobile node is moving based on the mobility data files that had been generated through mobility generator module. A quantity of 100 nodes are created. The transmission range is fixed at 100 meters. 100 nodes have destinations and check out finding routes to their destination nodes. Maximum speed of node is set to 20m/sec. The nodes are assigned with an initial position. All nodes do not discontinue moving and the simulation time is 500 seconds.

TABLE 1. SIMULATION PARAMETERS

Parameter	Value
Coverage area	500x500
Simulation Time	500ms
No of Nodes	100
Traffic Type	UDP-CBR
Packet Size	512 Bytes
Maximum Speed	2 m/s
Routing Protocol	MDSR
Mobility model	Random way point
Antenna Type	Omni antenna

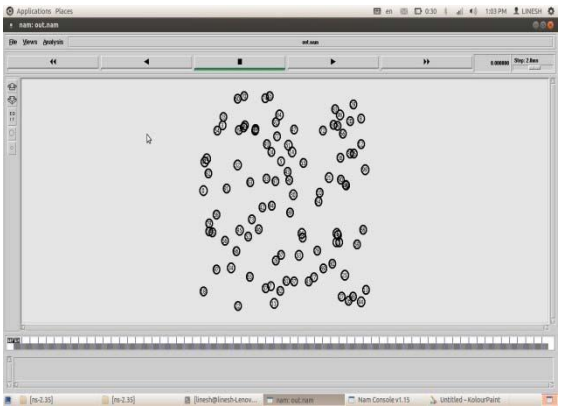

Fig 5. Initial position of the nodes

B. Modified DSR

In MANET, routing protocols should be designed giving prior attention to security and data integrity [8]. Modified Dynamic Source Routing (MDSR) is one such routing protocol that incorporates SNuPM algorithm which continuously monitors the behaviour of nodes in the network. AMN algorithm identifies the malicious nodes present in the network with the following assumptions.

C. SNuPM Algorithm

In this algorithm, Packet Drop Ratio and Energy level are the important parameters to compute the performance of a network. In this paper a node is inactive or vulnerable to attack when it's packet Drop ratio and energy level drops down below a threshold value. Trust based IDS works as the following assumption of calculating PDR (packet Drop ratio) and energy level.

Case 1: Energy Level Computation

Every node in the network is assigned with some initial energy value. The energy of a node is reduced for every transmission and reception of packets. The difference between the initial energy level and obtained energy level gives the final energy level of the node. If the energy level goes beyond 40% then the node is considered to be vulnerable to attacks and such nodes are noted. So continuous monitoring of node's energy has been carried out throughout the simulation.

Power Consumption

Every node in the MANET computes its power consumption for every transaction and finds the remaining energy periodically. Each node may operate in any of the following modes [9].

a) Transmission mode: The power consumed for transmitting a packet is given by Eq. (1)

$$\text{Consumed energy} = Pt * T \quad (1)$$

Where Pt is the transmitting power and T is transmission time.

b) Reception mode: The power consumed for receiving a packet is given by Eq. (2)

$$\text{Consumed energy} = Pr * T \quad (2)$$

Where Pr is the reception power and T is the reception time.

The value T can be calculated as

$$T = \text{Data size} / \text{Data rate} \quad (3)$$

Hence, the remaining energy of each node can be calculated using Eq. (1) or Eq. (2) based on the mode of operation.

Remaining energy = Current energy – Consumed energy……..(4)

Other two modes like sleep and idle are not considered in our proposal since energy reduction is negligible. Initially every node has full battery capacity say 100% which is assigned to current energy[10] .On each transmission or reception of a data packet the remaining energy is found using the Eq.(4). If the remaining energy falls below 40%, that node will not act as a router to forward the packets.

Case 2: Packet Drop Ratio Computation

When packets are forwarded from source to destination the quantity of dropped packet can be estimated by the following formula.

Packet delivery ratio=(Nr/Nf)*100

PDR=No. of packets generated – Packet delivery ratio.

Where, No. of packets forwarded to destination = Nf, No. of packets received at destination = Nr, Probability of Packets received =Pr [11].

Case 3: Confirmation of Malicious Behaviour

Malicious nodes are nodes which do not meet the requirements and overcome the network protocol [12]. From the above two cases calculated, If energy level is less than 40% and packet drop ratio is greater than 20 % for a particular node then the node is demonstrated to be a node that cannot effectively involve in transactions anymore and mismatches the protocol or simply called a malicious node. From results obtained by above two tables the node with minimum energy level (i.e, less than 40%) and PDR (greater than 20%) is to be treated with Promiscuous mode. This will lead to the re-enforcement (which converts them back into a normal node after a periodic interval by local repair scheme) of such nodes that will certainly increase the energy level of the node and the capacity to transfer packets in Trust based IDS.

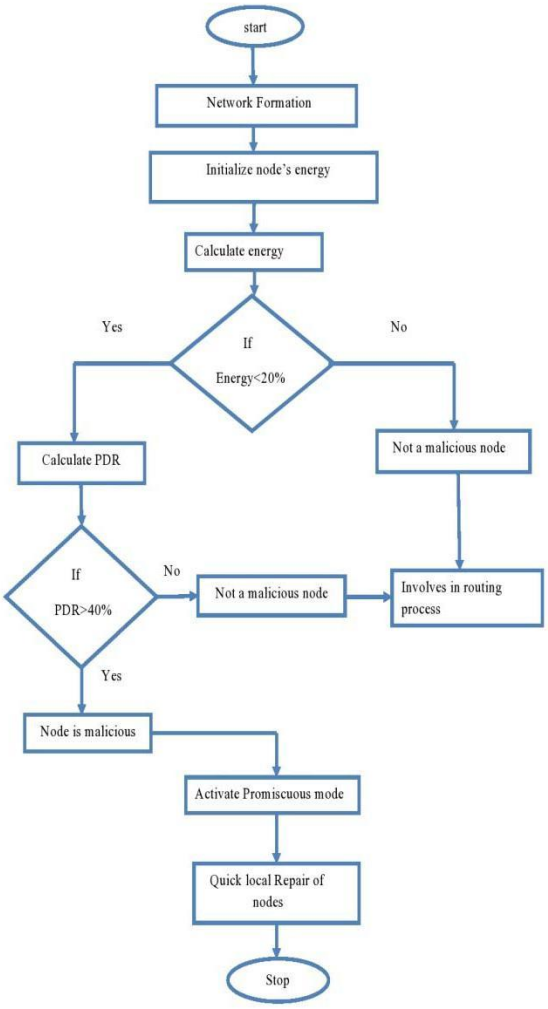

Fig 6. Flow chart for Promiscuous mode

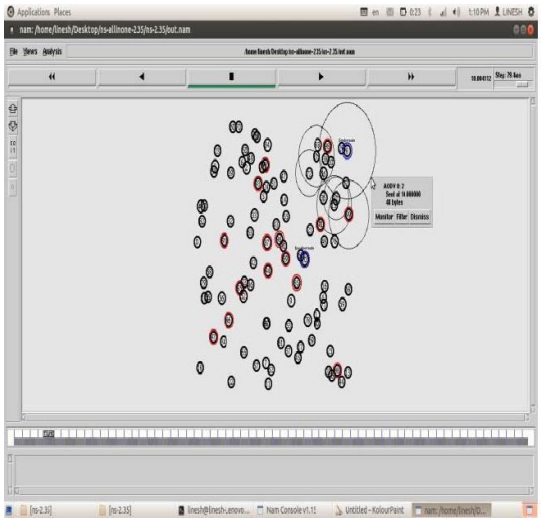

Fig 7. Path Optimization by Detecting Malicious Nodes in MDSR

Figure 6 demonstrates how malicious nodes are detected and treated with Promiscuous mode to convert them back into a normal node in a stipulated time. This continuous monitoring of nodes in a network will possibly increase the efficiency of the network. Since the nodes are treated and made to participate again in the routing process the entire lifetime of the network is increased. However, the efficiency of the network depends upon how the nodes actively perform in the network after its recovery

VI. PERFORMANCE ANALYSIS

Throughput and PDR are considered to be the major parameters to enhance the performance of the entire network [7]. Here, MDSR is proposed to enhance the overall quality of service of the network. PDR and Throughput are computed with the following formulas:

Packet delivery ratio= (Nr/Nf)*100.....(5)

PDR=No. of packets generated – Packet delivery ratio.

Where, Nf= No. of packets forwarded to the destination

Nr= No. of packets received at the destination

Throughput = Number of Packets sent / time.....(6)

```
void MalTimer::handle(Event*) {
agent->check_mal();
Scheduler::instance().schedule(this,&intr,0.5);
}
void DSR::check_mal() {
if(index==0) {
if(fcount > rcount +1) {
fprintf(stderr, "No. of packets dropped are %d\n",fcount-rcount);
  }
 }
}
```

Fig 8. To Estimate Run-time Packet Drop

```
#filename:Throughput.awk

#---- Formula ----:

Throughput = received_data*8/DataTransmissionPeriod

#---- AWK script Format---#
The script has the following format:
BEGIN {}
{
content
}
END {}
```

Fig 9. To Calculate Throughput

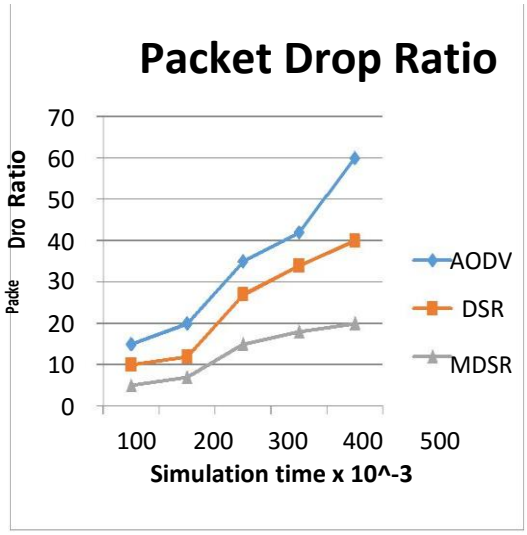

Fig 10. Comparison of Packet Drop Ratio between DS AODV and MDSR

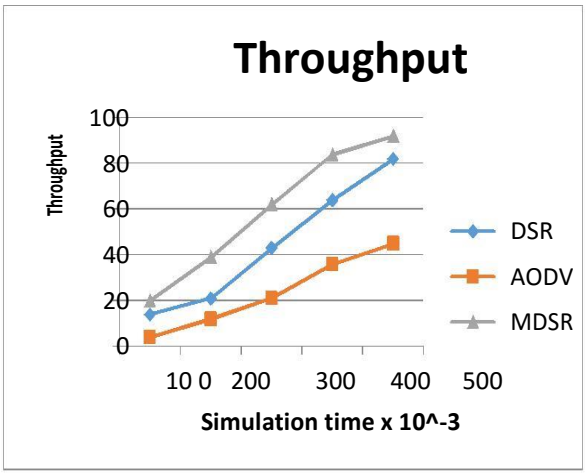

Fig 11. Comparison of throughput between DSR, AODV and MDSR.

From the above graph, it is inferred that the PDR has been reduced drastically since there is no any malicious node participated in the routing process. Similarly, throughput is also maintained uptime throughout the routing process. This inference shows that the proposed method is far better that the existing methods to improve the efficiency of the network by eliminating the malicious nodes.

VII. CONCLUSION

The reliability of the network is a major concern that should be concentrated to improve the efficiency and Quality of Service of the network. MANET, as it is more vulnerable to attack this paper proposes a mechanism called Promiscuous mode that converts the malicious node into a usual node. Promiscuous mode has local repair scheme that is used to convert the nodes to normal state to initiate its configuration in network again. So, the Promiscuous mode is initiated that monitors such inactive nodes and convert them into active one. Our future work is to implement IDS mechanism for all threats in MANET by incorporating Trust evaluation and management as Trust based IDS.

REFERENCES

[1] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad-hoc Networks, ACM Proceedings, (2003).

[2] Sun, Bo, et al., Intrusion detection techniques in mobile ad hoc and wireless sensor networks. IEEE Wireless Communications 14 (5): 56-63 (2007).

[3] Gurnam Singh and Gursewak Singh, Improvement of Network Efficiency by Preventing. IJITEE 4(2): July (2014).

[4] Dilpreet Kaur and Naresh Kumar, Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV routing protocols in Mobile Ad-hoc Networks. J. Computer Network and Information Security 3: 39-46 (2013)

[5] Parma Nand and Dr. S.C. Sharma, Routing Load Analysis of Broadcast based Reactive Routing Protocols AODV, DSR and DYMO for MANET. International Journal of Grid and Distributed Computing 4(1): 81-91 (2011).

[6] S. A. Ade and P.A.Tijare, Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad-hoc Networks. International Journal of Information Technology and Knowledge Management 2(2): 545-548 (2010).

[7] P Johansson, T Larsson, N Hedman et al., Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks. Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking. ACM, (1999).

[8] S Marti, TJ Giuli, K Lai and M Baker, Mitigating Routing Misbehavior in Mobile Ad-hoc Networks, Proceedings of 6th international conference on Mobile computing and networking. ACM (2000).

[9] M. Pushpalatha, RevathiVenkataraman, and T. Ramarao, Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad-hoc Networks. World Academy of Science (2009).

[10] Pirzada, Asad Amir, and Chris McDonald. Secure routing with the AODV protocol. Asia-Pacific Conference on Communications. IEEE (2005).

[11] Semih Dokurer and Y.M. Erten Acar, Performance Analysis of Ad-hoc Networks Under Selective Black hole Attacks, Proc: of the IEEE SoutheastCon, pp.148-153 (2007)

[12] Kannhavong, Bounpadith, et al., A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications 14(5): 85-91 (2007).

[13] Kang, Nan, Elhadi M. Shakshuki, and Tarek R. Sheltami, Detecting misbehaving nodes in MANETs. Proceedings of the 12th international conference on information integration and web-based applications & services. ACM (2010).

[14] Komninos, N., Vergados, D. and C. Douligeris, Detecting unauthorized and compromised nodes in Mobile Ad-hoc Networks. Ad Hoc Networks 5: 289-298 (2007)

[15] Nidal Nasser and Yunfeng Chen, Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad-hoc Networks, IEEE Communications Society subject matter experts for publication in the ICC proceedings (2007).

[16] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami EAACK—A Secure Intrusion-Detection System for MANETs. IEEE Transactions on Industrial Electronics 60(3): 1089-1098 (2013).

[17] L. Tamilselvan, Latha, and V. Sankaranarayanan, Prevention of co-operative black hole attack in MANET. Journal of Networks 3(5): 13-20 (2008).