International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 3 (2018) pp. 1605-1612

Design and Evaluation of MANET attack model with DSR routing protocol

[1] Arage Chetan S and [2] Satyanarayana K V V.

[1,2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur-522502, Andhra Pradesh, India.

Abstract

MANET is one of widely used unsecured open nature wireless networks in small to large real time applications. The open nature of such network leads to possibilities of both inside and outside security threats for important communications in MANET. As we aware that, MANET is not having any fixed topology and mobile nodes are moving randomly in network, this also leads to the possibility of security threats in network. The solutions for network security in MANET is designed and evaluated with goal of QoS efficiency while defending against the MANET security threats like malicious user attack, black hole attack etc. The goal of this paper is not to present another security solution based on routing protocol for MANET, rather our aim is to design the MANET routing attack model and its simulation with well known routing protocol DSR by considering with and without attacks in network. This study will gives us the impact of MANET routing attacks on routing performance and identification of areas in which efficient mitigation should be performed through the extensive NS2 based simulation.

Keywords: Mobile ad hoc network, Routing, Security, Wireless Communications, Wireless Network

INTRODUCTION

The ad-hoc means short term and Mobile means 'moving' without the infrastructure. So, the mobile ad-hoc network is created the sets of mobile nodes, these collaborate to communicate with each other nodes externally any fixed central base station [1]. The mobile ad hoc network (MANET) is also known as mesh mobile network, these are the network of electronic (mobile) devices join by the wireless links. The MANET is also called as the temporary network. In the temporary network, the mobile devices are composed separately on another mobile nodes, these node are similar in the wireless network. The mobile nodes in wireless network are moving rapidly in overall wireless network. The MANET networks are mainly created for temporary wireless networks and these networks does not necessary of infrastructure for deploying administration and deploying. The mobile nodes communication are totally based on the routing algorithm, these are used known as multi-hop routing protocols. These protocols are main functionality of sending the data packet from sender mobile number to the expected receiver. In the wireless networks each and every mobile node is working on the forwarding node and host node. The forwarding nodes meaning are the routing algorithm functionality and operation. The another meaning are, the routing algorithm (protocol) for the mobile ad hoc network are invented for foundation the wireless communication network and communication router. The infrastructure of dynamic communication a route in the overall network is over between the starting node to ending node for communication purpose on demand way and hence these are the main task of MANET routing protocols [2].

The mobile ad hoc networks does not stable network topology required to the cause that nodes are rapidly modify their movement and position. Mobile ad hoc networks having are various kinds of routing algorithm (protocols) these are hybrid, proactive protocol and reactive [3]. So we are used these algorithm (protocol) with various network structure and versatility pattern. The reactive protocols thus are as Ad hoc on demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) are commonly used for MANET protocols. The examples of the reactive protocol are Optimized Link State Routing (OLSR) and Sequenced Destination Vectoring (DSDV). The hybrid protocol is the various kinds of protocols thus are ZRP (Zone Routing Protocol). These protocols are used in the mobile ad hoc networks. Required to the defective, malicious, virus and self central nature of mobile nodes are outcomes in to deviates node. The any types of the hardware or software defects are responsible for defective nodes. The self central nodes are taking the inputs from the other nodes in the mobile network but do not send to another sending node and these are fall these data packets [4]. The Malicious node in the mobile network accepted another nodes into the incorrect direction enough that the knowing direction by published data that that he has smallest path for knowing recipient of data. This attack is known as DoS attack. The all receive data packet fall by the defective node. The black node attacks are defective performance of the nodes outcomes in to the falling data packets. That due to these types of attack, MANET network becomes the unprotected for the performance serve of used routing protocols. These are multiple explanation are invented for addressing this wireless networks attacks and still the researches are going on. But we use the routing protocols for the mobile network that can be affected on throughput and performance degradations for these mobile networks [5].

Thus in such conditions we need to have good IDS (intrusion detection system) mechanism in place to secure the wireless networks. Recently in literature we have studied the different methods presented by different authors to identify and mitigate the attacks over MANET. However each method is suffered from limitations like when group mobile attackers performing the collaborative attack on MANET, existing methods such as EAACK [1], 2ACK [2] etc. performing worst to recognize and protect thus attack.

In this research paper are, presenting the study on design of attack model and its evaluation with reactive routing protocol called DSR. DSR is one of widely used routing method for

MANET communications [6]. In this paper, we redesign the DSR routing protocol with addition of attack model in order to monitor and evaluate the impact of security threats on DSR routing protocol. In section II, the study on previous recent studies on MANET attacks and its evaluation is presented. In section III, the summary of DSR routing protocol is presented. In the section IV, that attack framework is represented. In section V, simulation results and its discussion is presented. Finally conclusion is reported in section VI.

RELATED WORK

In [6], Vaishali Desai conducted the analysis on the accountability of the OSLR (Optimized Link State Routing) protocol while this research paper. The routing table overflow attack and link spoofing attack are imitation by researches on the Optimized Link State Routing protocol. The severances were determined by differentiates routing attack opposite throughput of OLSR protocol.

In [7], Kranthi Kumar introduced enhanced edition of exude detector technique as well as repetitive examining technique to perceive conspire harmful nodes; administrations of path in wireless multi hop networks. Exude detector authorize the computation of packet-loss ratio for separate nodes. Repetitive examining authorizes dependable detection of self-centered nodes which fall packets in a MANET.

In [8], Sukiswo introduced a MANET network utilizing Ad Hoc on-demand Multipath Distance Vector (AOMDV) routing protocol. In that network they established rushing as well as swamping ambush. 3 frameworks utilized in this research collected, such as network situations revealed rushing attacks, flooding attacks as well as rushing with flooding attack respectively.

In [9], Kuldeep Singh presented study on different attacks and their impacts of MANET routing. The attacks impact was studied on the protocols using parameters like Normalized Routing Overhead, Packet Delivery Ratio, Throughput, Packet Loss, Mean Hop Count as well as End to end delay.

In [10], Raj Kamal Kapur claimed that how it is imperative to study the vulnerabilities of the routing protocols and methods of launching the attack in detail. They presented and report several present literature on reduction of the routing attacks conceptually.

In [11], Apoorva Chandra presented simulation and evaluation of performance of ZRP (zone routing protocol), AODV (adhoc on demand distance vector protocol) and HWMP (hybrid wireless mesh protocol) opposite to gray hole, black hole and jellyfish reordering attacks these reversely effect the services of protocols. Though for MANET multiple numbers protocol and improve protocols has never been check to multiple numbers network attack. The throughput analysis shown had quantitatively denoted facts; these are used for particular routing protocols. They evaluated the routing protocols those are used newly by mobile devices and these depend on research hybrid protocols, reactive protocol and proactive protocol. The function shown in specific node scheme against the vulnerabilities which they are shown.

In [12], Sagar R Deshmukh presented this was another approach for secure routing algorithm to recognize and drop black hole attack and that impact on routes in the starting stage of routes finding using AODV routing protocol. An effective value was connecting to RREP which secure that their attacks on the path. This approach was simulated in network simulator 2 and analysis of throughput

In [13], Lineo Mejaele introduced the analyses over the throughput of DSR and AODV when attacked by black hole, by changing the versatility of the mobile nodes in the network. The examiner was performing by imitation scheme of DSR and AODV based MANET using NS-2 with the black hole attack in which of the scheme. The various scheme were designed by modify the mobility of the mobile nodes.

In [14], Houda Moudni simulated the black hole, flooding and rushing attacks these are warning in AODV (Ad hoc On-demand Distance Vector) protocol in manner to examine their affects on this protocol by using NS-2 network simulator. Author claims that earlier methods taken one attackers or the mobility to check there throughput evaluation, hence they conducted evaluation on the mobile network size, load of traffic, mobility and multiple number of attackers. They can be use data packet delivery ratio and throughput for a performance analysis metric. The output declared that black hole attack extreme affects on the network throughput while the flooding and rushing attacks are very low importance impacts on the network performance

In [15], Jayashree S Patil introduced an integrated technology for attack auditing and risk evaluation in MANET routing. These innovation technique take a few node thus are auditing nodes using Gittins index. The auditing node is responsible for analysis and finding the risk in nodes. The risk is recognizing in node then analysis reputation values and accurately, the warning message was sending to node to implore the risk evaluation process.

In [16], Lakshit Prashar presented another study on MANET attacks and their evaluation DSR and AODV routing protocol is presented by author. Their objective was to check the impact of black hole and wormhole attacks on AODV and DSR protocols.

In [17], Ram Kishore Singh introduced the literature report paper on routing algorithm (protocols), these protocol are DSR and AODV. They presented various attack performance and preventive against these attacks are, Greyhole attack, Black hole attack and wormhole attack.

DSR MODEL

In this section, brief summary for DSR protocol.

Advantages

1. Trivially loop free nature of source routing by route information inspection
2. Caching routing information from packets forwarding (ease dropping)
3. Routes established on demand lend to scalability

Phases of DSR

Route Discovery

This process occurs when a node necessary to forwarding a

message to other node this path of nodes is already known. It is composed of below mentioned list of steps:

1. Multiple replies are cached for future use
2. Caching reduces work on new route requests
3. Source and destination in RREQ header
4. Route record is initialized as empty list
5. Unique route request ID, Hop Count
6. If Relay node sees its own address or request ID in RREQ then discarded otherwise it is broadcast with its own address
7. Relay nodes examine local cache for shorter route, if not it rebroadcasts adding its address to path
8. Route Reply RREP contains outbound path info but may need to determine how to get message back to source (asymmetric problem).
9. If it performs a RREQ to the original sender, it will piggy backs the initial RREQ on its own route discovery (RREQ).
10. Are stored in sending buffer until a route is discovered
11. This buffer fills and can wait for some time out before deleting the packet
12. The buffer may act as a circular queue
13. As packets remain in queue perform a new route discovery, cached routes deleted on time outs or route error replies

Route Maintenance

1. Somewhat alluded to above: Packet retries, route error RERR responses
2. Send buffer is full causes use of other cached routes, if routes don't work they are pruned
3. If no cached routes found Route Discovery performed

Error Recovery

1. RERR messages are used to update cache where link errors have occurred Intermediate links update their cache.

ATTACH MODEL

This section presents the design for normal and attack based models and their difference in working in MANET routing. The security threats in MANET allow attacker to compromise the original nodes in order to make then malicious.

Normal Behavior

The normal behaviour wireless node means such node is supporting the wireless operations in MANET like transmitting data from source node to intended receiver node via intermediate nodes/node while achieving security goals. The main security goals are Non-Repudiation (NP), Availability (Av), Authenticity (Au), Confidentiality (C), and Integrity (I). Figure 1 shows the normal nodes behaviour example to transmit data from S to D via N1, N3 and N4 nodes.

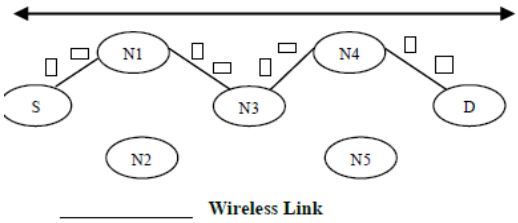

Figure 1. Example of Nodes Normal Behavior

Malicious Behavior

If the node is affected by any type of security threats is then treated as attacker and malicious node in network. The properties of such mobile nodes are either of listed below:

1. Malicious mobile node can receive and drop the incoming data packets relatively than sending to other node.
2. Malicious node performs redundant activities with goal of energy consumption in network.
3. The fake packets update leads to buffer overflow problem in network. The buffer overflow leads to no space available for legitimate updates.
4. Unnecessarily bandwidth utilized by malicious nodes so that legitimate nodes failed to use it.
5. Such nodes can enter in network without any authentication process.
6. Insertion of stale packets in wireless network with objective of creating the confusion in such network.
7. Malicious nodes delaying the process of packet forwarding purposefully.
8. Frequent route breaks in MANET leads to information loss, QoS loss. Malicious nodes can perform the frequent link break operations if it is intermediate node between source and destination.
9. Malicious nodes can compromise or tamper the packets data.
10. Malicious nodes may deny from sending the data to other legitimate wireless nodes in network.
11. Fake routing generation is another property of malicious nodes. Malicious nodes can show the fake paths to source nodes to receive the packets and misuse it.
12. The malicious node isolates any legitimate node from taking the part of any process in order to create the delays in communication.
13. Malicious behavior may include the information stealing. The information which can be steal information like location, content, sequence number etc.
14. Whenever two normal nodes exchanging data, malicious node may capture their session with aim of collecting important information.
15. Apart from this, there are some other methods or characteristics through the malicious activities may perform by malicious nodes.

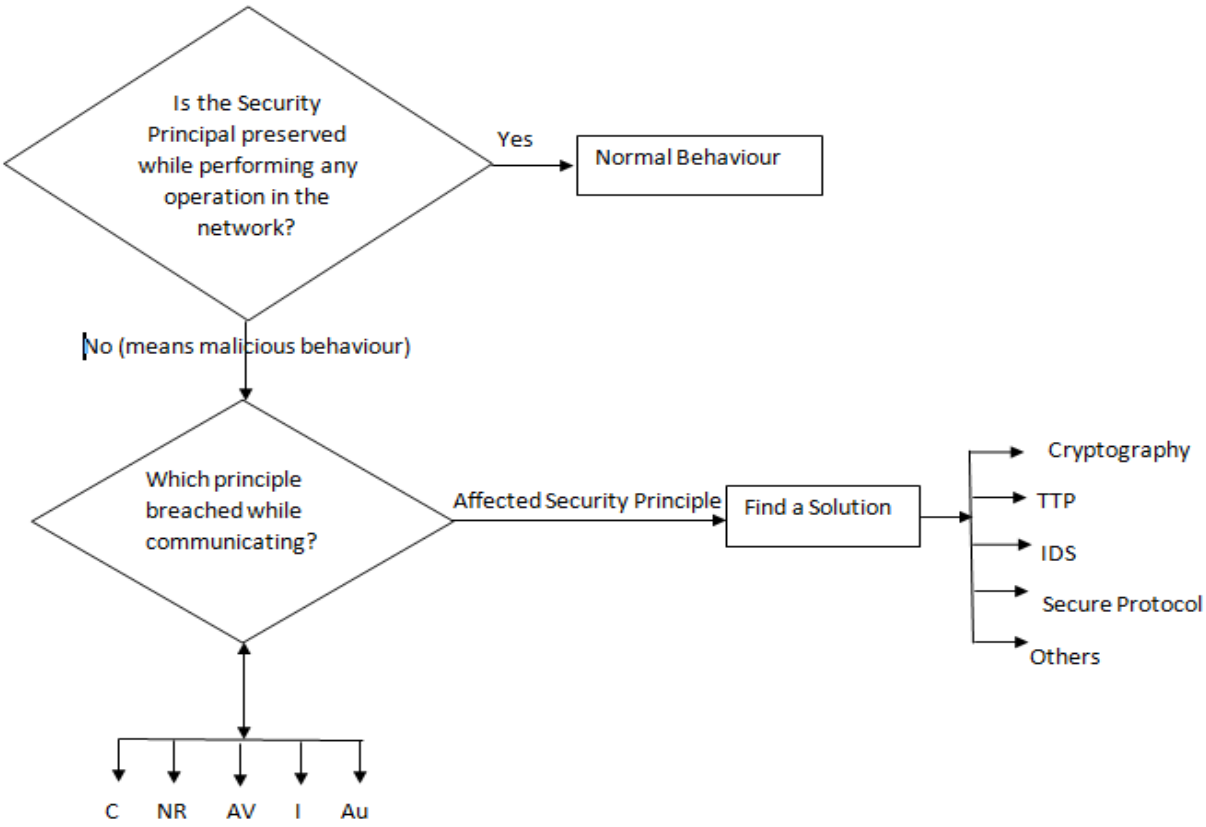

Figure 2. Model for Normal and Malicious Node Behavior

Figure 2 explaining the behavior of both normal and malicious wireless nodes in MANET.

We modified the DSR routing protocol to introduce the malicious behavior on nodes of our choice in order to track the impact. This can be represented in below simple steps:

1. Input: name of node to be performed as malicious
2. Reading node name
3. RREQ ()
4. RREP ()
5. RRER ()
6. If its malicious

[1] Drop Packets ();

[2] Else

[3] Forward Packets

Stop

SIMULATION RESULTS

The simulation and evaluation is done using NS2. There are two scenarios we considered while designing networks such varying percentage of malicious nodes in network and mobility speed.

Scenario 1: Varying Malicious Nodes

Table 1 is showing the parameters used to design such networks. Figure 3, 4 and 5 are showing the results for throughput, delay and PDR among normal DSR and Attack based DSR protocol. From the results it is clear that as the attackers increases their significant performance drop in all three parameters. Throughput and PDR gets worst or minimum and delay gets increasing with increase of total number of malicious users in network. This clearly shows the how malicious nodes impact on routing performance.

Table 1: Network Parameters

Number of Nodes	50
Traffic Patterns	CBR
Network Size (X * Y)	1000 x 1000
Max Speed	10 m/s
Simulation Time	50s
Transmission Packet Rate	10 m/s
Pause Time	1.0s
Routing Protocol	DSR
MAC Protocol	802.11
Channel Data Rate	11 Mbps
Number of Malicious Nodes	0 %-40 %

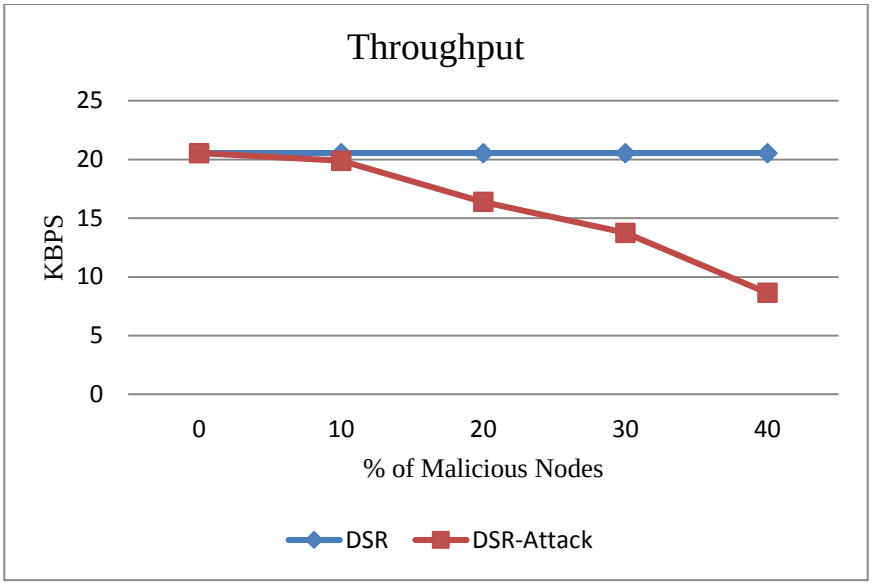

Figure 3. Throughput Performance Analysis for Scenario1

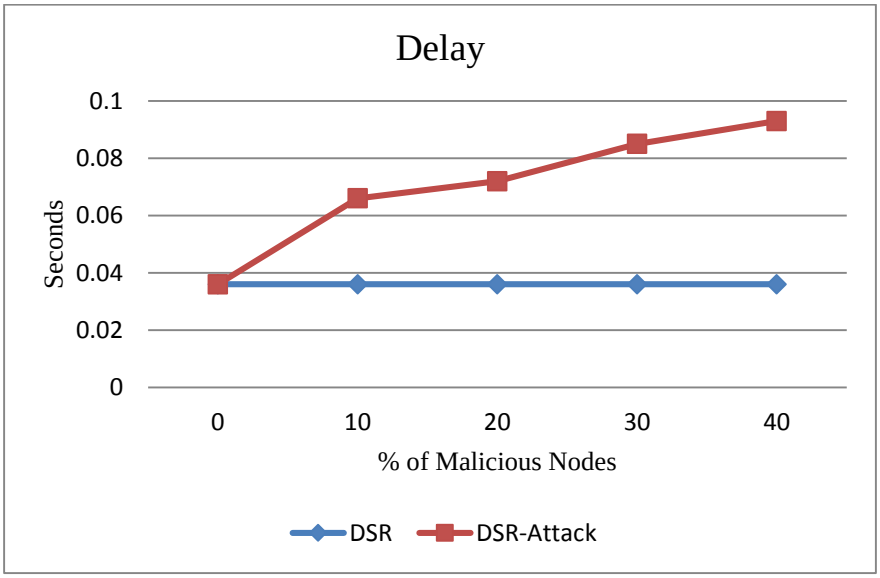

Figure 4. Delay Performance Analysis for Scenario 1

Scenario 2: Varying Mobility Speed

Apart from the varying number of attackers, mobility is also having major role in routing performance under presence of attackers in network. Below properties we used for this scenario in simulation:

Routing Protocols: **DSR and DSR-Attack**

Number of wireless nodes: 50

MAC: 802.11

Simulation Time: 30 Seconds

Speed of Mobility: 5, 10, 15, 20, 25 (m/s)

Number of Attacks: 2

Figure 6, 7 and 8 showing the results for this scenario respectively for throughput, PDR and Delay analysis. From the results it shows, there is impact of presence of malicious users in network. Also it shows that as the increasing the mobility speed, the impact of malicious node is getting lower on the PDR and throughput performances, but the delay performance becoming the worst.

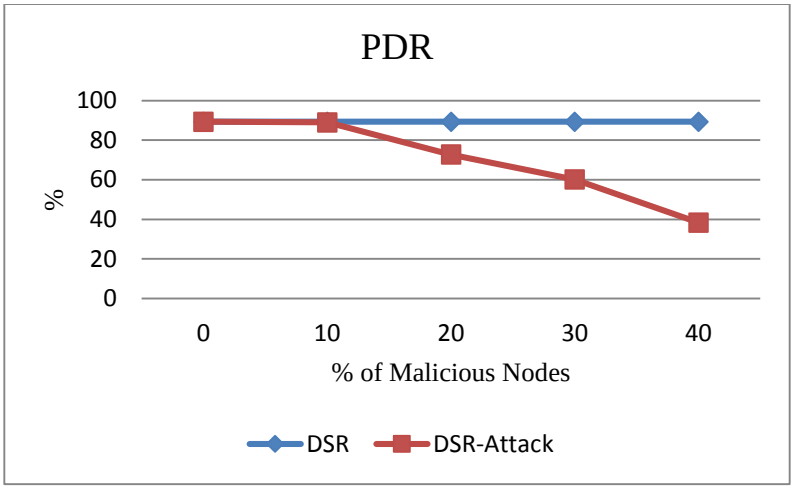

Figure 5. PDR Performance Analysis for Scenario 1

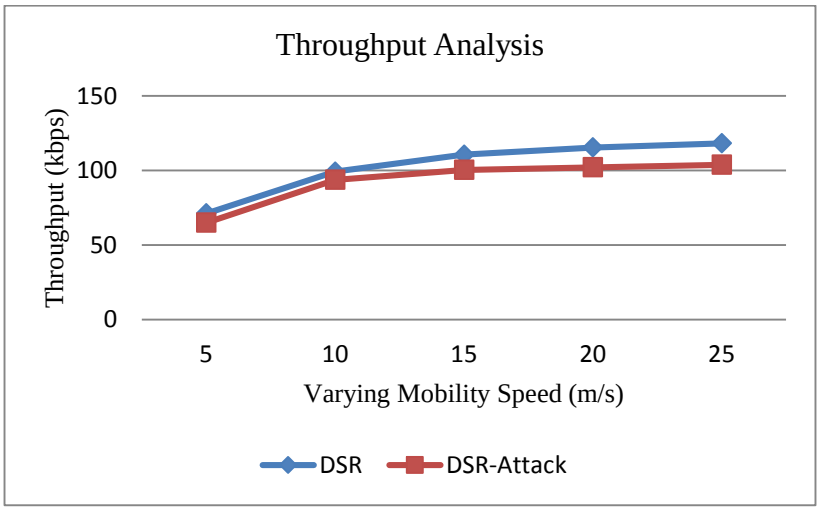

Figure 6. Throughput Performance Analysis for Scenario 2

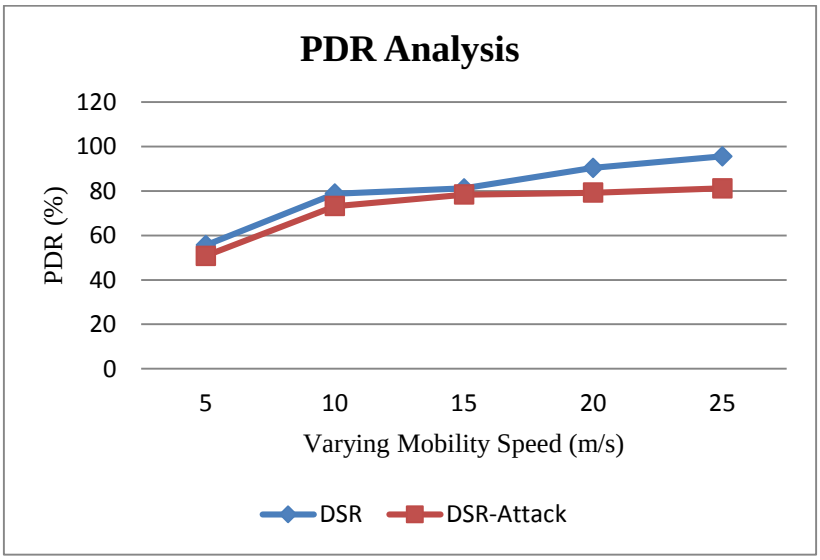

Figure 7. PDR Performance Analysis for Scenario 2

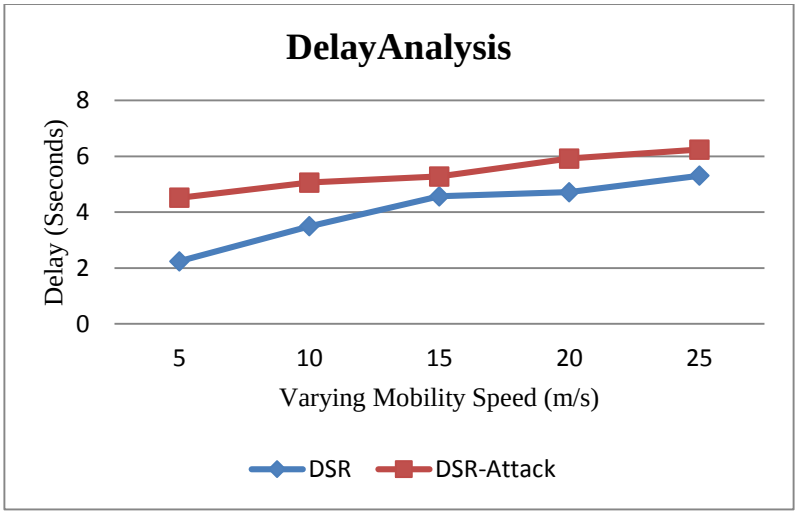

Figure 8. Delay Performance Analysis for Scenario 2

CONCLUSION AND FUTURE WORK

In this paper, the review is presented on evaluation and study over security attacks in MANET routing protocols. Then we presented the DSR summary as we further modified the DSR protocol with inclusion of malicious nodes behavior. The performance evaluation is done by considering the two different network scenarios one with varying number of malicious users and another with varying mobility speed with two nodes acts as attackers. The simulation result shows the impact of malicious users in network. In future, we will study the different routing security methods and present current research gap.

REFRENCES

[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions On Industrial Electronics, VOL. 60, NO. 3 MARCH 2013 doi: 10.1109/PERVASIVE.2015.7087032 .

[2] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007 doi 10.1109/TMC.2007.1036.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw. Boston, MA, 2000, pp. 255–265 doi:10.1145/345910.345955.

[4] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009 doi:https://doi.org/10.1007/s00530-009-0166-0.

[5] R. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007 doi:10.1109/TMC.2007.1036.

[6] Vaishali Desai, Narendra Shekokar, "Performance Evaluation of OLSR Protocol in MANET under the Influence of Routing Attack", 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN) doi:10.1109/GCWCN.2014.7030865

[7] Kranthi Kumar. K, Vasantha Laxmi .CH, K. Srinivasa Rao, "Identifying the Behavior: Nodes, Route and Collusion Attack's in MANET", 2014 IEEE International Conference on Contemporary Computing and Informatics (IC3I) doi:10.1109/IC3I.2014.7019683

[8] Sukiswo, Muhamad Rifqi Rifquddin, "Performance of AOMDV Routing Protocol Under Rushing and Flooding Attacks in MANET", Proc. of20l 5 2nd Int. Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), Indonesia, Oct l6-l8th doi: 10.1109/ICITACEE.2015.7437835

[9] Kuldeep Singh, Amanat Boparai, Vrinda Handa, Prof. Sudesh Rani, "Performance Analysis of Security Attacks and Improvements of Routing Protocols in MANET",2015(CSCESM) doi:10.1109/CSCESM.2015.7331887

[10] Raj Kamal Kapur, Sunil Kumar Khatri, "Analysis of Attacks on Routing Protocols in MANETs", 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) MS Engineering College, Ghaziabad, India doi: 10.1109/ICACEA.2015.7164811

[11] Apoorva Chandra, Sanjeev Thakur, "Performance Evaluation of Hybrid Routing Protocols Against Network Layer Attacks in MANET", 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun,

India, 4-5 September 2015 doi: 10.1109/NGCT.2015.7375119

[12] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople, "AODV-Based Secure Routing Against Black hole Attack in MANET", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India doi:10.1109/RTEICT.2016.7808179

[13] Lineo Mejaele*'v and Elisha Oketch Ochola, "Effect of Varying Node Mobility in the Analysis of Black Hole Attack on MANET Reactive Routing Protocols", Information Security for South Africa (ISSA), 2016 doi: 10.1109/ISSA.2016.7802930

[14] Houda Moudni, Mohamed Er-rouidi, HichamMouncif, Benachir El Hadadi, "Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks", 2nd International Conference on Electrical and Information Technologies ICEIT'2016 doi:10.1109/EITech.2016.7519658

[15] Jayashree S Patil, Dr.K.V.N.Sunitha2, "A Combined Technique For Attack Monitoring and Risk Assessment In MANET Routing", 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN) doi:10.1109/WOCN.2016.7759890.

[16] Lakshit Prashar, Raj Kamal Kapur, "Performance Analysis of Routing Protocols under Different Types of Attacks in MANETs", 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) doi: 10.1109/ICRITO.2016.7784989

[17] Ram Kishore Singh, Parma Nand, "Literature Review of Routing Attacks in MANET", International Conference on Computing, Communication and Automation (ICCCA2016) doi: 10.1109/CCAA.2016.7813776

[18] K. Osathanunkul, N. Zhang, "A countermeasure to black hole attacks in mobile ad hoc networks", Networking Sensing and Control (ICNSC) 2011 IEEE International Conference *On*, pp. 508-513, 2011 doi: 10.1109/ICNSC.2011.5874910.

[19] N. Sharma, A. Sharma, "The black-hole node attack in MANET", Advanced Computing & Communication Technologies (ACCT) 2012 Second International Conference On, pp. 546-550, 2012 DOI: 10.1109/ACCT.2012.112.

[20] P. K. Singh, G. Sharma, "An efficient prevention of black hole problem in AODV routing protocol in MANET", Trust Security and Privacy in Computing and Communications (TrustCom) 2012 IEEE 11th International Conference On, pp. 902-906, 2012 DOI: 10.1109/TrustCom.2012.78.

[21] R. Agrawal, R Tripathi, S. Tiwari, "Performance evaluation and comparison of AODV and DSR under adversarial environment", Computational Intelligence and Communication Networks (CICN) 2011 International Conference On, pp. 596-600, 2011 DOI: 10.1109/CICN.2011.129.