International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 7777-7788

http://www.ripublication.com

Impact of Malicious Nodes in Mobile Adhoc Networks

[1]J.V.Anchitaalagammai, [2]N.Uma Maheswari, [3]R. Venkatesh

[1]Department of Computer Science and Engineering, Velammal College of Engineering and Technology, Madurai, Tamil Nadu 625009, India, anchithaalagammai.dss @gmail.com

[2]Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu 624622, India

[3]Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu 624622, India

Abstract

Mobile Adhoc networks (MANETs) are highly dynamic networks lacking physical infrastructure. Network nodes function as routers discovering and maintaining routes with other nodes. Mobility leads to network connections changing dynamically with nodes being added/removed any time. In this paper, the effect of malicious nodes on MANETs performance is investigated. Malicious nodes mimic normal nodes but deliberately drop packets to conserve energy. In this work, the impact of malicious nodes is observed in MANET for DSR routing protocol. The experimental setup consists of 25 nodes distributed over two square kilometers. Three experiments are conducted the first network without malicious nodes and with 2% and 5% of the nodes being malicious.

Keywords: Mobile Adhoc networks (MANET), Dynamic Source Routing (DSR), Malicious Nodes, Attacks, Selfish Node

1.INTRODUCTION

Mobile Adhoc networks (MANET) are collection of mobile devices (nodes) communicating with each other without a predefined infrastructure/centralized administration [1]. MANETs are continuously self-configuring due to the dynamic nature of the nodes. A MANET in addition of freedom of mobility, can be constructed quickly at low cost, as it needs no network infrastructure. Hence, a MANET is attractive for emergency operations, disaster relief, maritime communications,

military service, vehicle networks, campus networks, casual meetings and robot networks. Unlike conventional networks, MANETs are characterized by dynamic, continuously changing network topology due to node mobility [2]. This feature makes it hard to perform routing in MANETs compared to conventional wired networks. Another MANET characteristic is its resource constraints like limited bandwidth and limited battery power [3]. MANETs are specifically vulnerable to attacks due to its characteristics like open medium, distributed cooperation, dynamic topology and constrained capability [4].

A path between a MANET source and destination nodes is established using route discovery process of routing protocol [5]. Once this is done, source node starts sending data packet to next node on the path; the intermediate node identifies next hop node to destination along established path and forwards data packet to it. This continues till data packet reaches destination node. To achieve the desired MANET operation, it is important that intermediate nodes forward data packets for all source nodes. But, a malicious node could decide to drop packets instead of forwarding them called ‘data packet dropping’ attack, or data forwarding misbehavior as compared to deliberate malicious behaviour, where overloaded nodes are unable to forward data packets or have low battery reserves; also nodes might be selfish, for example saving battery to process own operations.

Different routing protocols try solving routing issues in MANETs one way or the other. They can are classified into proactive routing and reactive routing, based on the time when a route is determined. In reactive routing, a routing protocol does not take initiative to find a route to destination, till required. It is also referred to as "on demand" as route paths are discovered when a source sends a packet to a destination for which source has no path. The protocol attempts to discover routes only "on-demand" by flooding the network with its query. Such protocols reduce control traffic overhead at the cost of increased latency in finding destination routes. Examples of such protocols are Adhoc On-demand Distance Vector (AODV), Dynamic Source Routing **(**DSR). DSR [6, 7] uses source routing instead of hop-by-hop routing, with each packet carrying a complete, ordered list of nodes in its header through which a packet must pass. The advantage of source routing is that intermediate nodes do not maintain up-to-date routing information to route the packets they forward, as packets themselves already have all routing decisions. This coupled with the protocol’s on-demand nature, eliminates periodic route advertisement and neighbor detection packets in other protocols. Proactive routing stores routing choices by periodic flooding to ensure accessible paths for nodes. This contributes to high overhead in the network.

Both reactive and proactive routing protocols are vulnerable to routing attacks as routing is based on assumption that all nodes cooperate to locate best path. So, a malicious node can exploit cooperative routing algorithms vulnerabilities and lack of centralized control to launch routing attacks. Specifically, on-demand (reactive) MANET routing protocols, like AODV [8] and DSR [7], were not designed to be

secure against malicious attacks as its dependent on simple implicit trust-your neighbors relationships [9].

Attacks are classified as passive and active attacks. In passive attacks, attackers do not disrupt normal routing; they listen to routing traffic to get valuable information. But, active attackers inject packets into the network, eavesdrop and try to compromise network resources by performing a Denial Of Service (DOS) attack [10]. Network layer attacks in MANETs are divided into passive and active attacks, as seen in Figure 1.

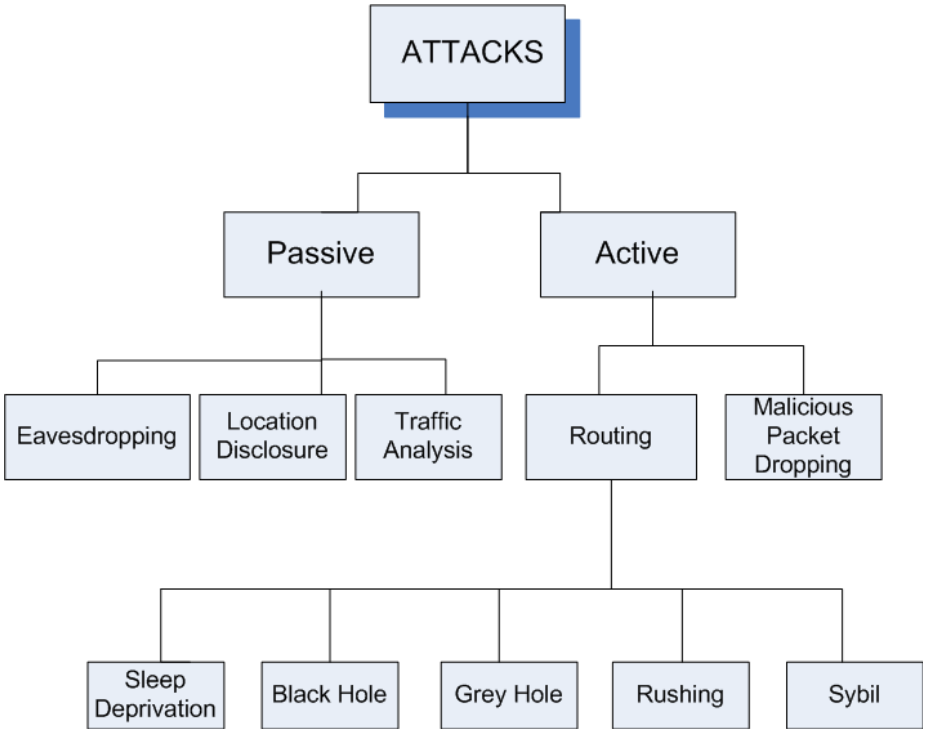

Figure 1 Classification of network layer attacks in MANETs

Passive Attacks: Passive attacks are those where attackers do not disturb routing protocol operations but try to seek valuable information through traffic analysis which leads to disclosure of critical network information or nodes like network topology, nodes location or important nodes identity. Examples of passive attacks are:

Because of MANETs wireless links, a message from a node is heard by every device within range which has a transceiver, and if encryption is not used then an attacker gets useful information. Senders and receivers have no way knowing that an attack has happened. Though eavesdropping is not considered to be a severe attack, it provides vital information in some scenarios and so researchers focus on minimizing it. For example in [11] authors analyzed risk of eavesdropping as a function of nodes transmission range and their geographical distribution.

Attackers listen to wireless links traffic to discover location of target nodes by analyzing communication patterns, amount of data transmitted by nodes and transmission characteristics. For example, in a battlefield, a huge amount of network traffic flows to and from headquarters. Traffic pattern analysis enables an intruder to discover networks commanding nodes. Even if data in a message is encrypted, traffic analysis can extract useful information. Though passive attacks do not directly affect network functioning, in some MANET application scenarios, like military communication, important information disclosure through traffic analysis/eavesdropping can prove costly. Examples of analysis and protection against such attacks are found in [12, 13].

Active Attacks: Intruders launch intrusive activities like modifying, forging, injecting, fabricating or dropping data or routing packets, resulting in various network disruption. Some attacks are caused by an intruder's one activity and others are due to a sequence of activities by colluding intruders. Active attacks (compared to passive attacks) disturb network operations and are so severe that they can bring down entire network or degrade network performance as in DOS attacks. So, this paper focuses on active network layer attacks. Active attacks are further divided into malicious packet dropping attacks and routing attacks, as seen in Figure 1.

But, due to adhoc networks increasing popularity some nodes act negatively in a network. These nodes are malicious nodes, undertaking attacks to jeopardize network resources. Due to MANET topology's dynamic nature and absence of infrastructure, they are vulnerable to attacks [14]. This node structure may disturb trust relationships among nodes. Lack of central points make detection of attacks difficult as it is hard to monitor traffic in dynamic and large scaled network [14]. All these MANET characteristics allow attackers to target network easily and salvage resources by disturbing/jamming communication between bona fide nodes. Malicious nodes perform adversarial attacks that damage the basic security aspects like integrity, confidentiality and privacy [15].

In this work, the impact of malicious nodes is observed in MANET for DSR routing protocol. The network performance such as throughput, end to end delay and retransmission attempts are evaluated for network without malicious nodes and with 2% and 5% of the nodes being malicious.

2. Related Works

Many research was conducted in MANETs security is available in the literature. Some schemes introduced new routing protocols that consider security and so they prevent some attacks. Other schemes were introduced to detect and deal with malicious nodes in the network.

Experiments for performance comparison of proactive and reactive routing protocols (AODV, DSR, DSDV and TORA) were performed by Broch et al., [16]. In simulation, a network of 50 nodes, 10 to 30 traffic sources, 7 different pause times

and various movement patterns was chosen. NS-2 discrete event simulator was used. Simulation led to the conclusion that DSR performance was good. AODV ensured more routing overhead than DSR at high node mobility.

A performance comparison of two on demand AODV and DSR routing protocols was presented by Das, et al., [17]. Simulation was through ns-2 simulator which supported an IEEE 802.11 MAC layer, a radio model similar to Lucent's Wave LAN radio interface and random waypoint mobility model where pause time varied from 0 to 900 seconds. Two scenarios were considered and different performance metrics computed for both protocols.

MANET network routing protocols DSDV, AODV and DSR were compared using network simulator NS2.34 by Tuteja, et al., [1]. They compared performance of three protocols together and individually. Performance matrix includes PDR, Throughput, End to End Delay and routing overhead. This paper compared performance of routing protocols when packet size changed, when time interval between packet sending changed and when node mobility changed.

A new mechanism called DARWIN (Distributed and Adaptive Reputation mechanism for Wireless adhoc Networks) was presented by Jos, et al., [18] which avoided retaliation when a node is falsely perceived as selfish to help restore cooperation. Using game theory, they prove that the new mechanism was robust to imperfect measurements, was collusion-resistant and achieved full cooperation among nodes. Simulations complement theoretical analysis and evaluated the proposed algorithm's performance compared to other reputation strategies.

Secured ZRP (SZRP) based on efficient key management, secure routing packets, detection of malicious nodes, secure neighbor discovery, and preventing nodes from destroying the network was proposed by Ravilla, et al., [19]. This paper suggests a new technique to deal with malicious nodes and prevent them from destroying the network further. This paper demonstrates SZRP performance using NS2 Simulator. It also compares performance of SZRP and ZRP considering performance metrics like Routing Overhead, Packet Delivery Fraction and End-to-End Delay. It also simulated performance at detecting malicious nodes using trust value and alarm packets. It observed that packet delivery fraction of SZRP was considerably high even when malicious nodes were 35% of Network size.

An attempt to study performance of two prominent MANET on demand reactive routing protocols DSR and AODV was proposed by Jain, et al., [20]. Though both share similar on-demand behavior, differences in the protocol mechanisms lead to significant performance differentials which are analyzed regarding throughput, packet dropped and packet lost. But, due to transmission nature in error prone shared wireless medium, nodes in communication range may behave selfishly. This paper analyzed reactive protocols in the presence of malicious nodes.

The concept of a new algorithm which is an enhanced version of the existing FACES Algorithm routing data based on trust was explored by Geethu, et al., [21]. Trust is evaluated by a Challenge scheme that isolates malicious nodes and also makes them trust worthy. A security solution for MANETs using AODV, and using password security for routing node and timeliness to update routing table was proposed by Suman, et al., [22]. AODV and Secure AODV (SAODV) are simulated and performance of both is evaluated for varying nodes and malicious nodes. Performance of SAODV was stable while AODV was degrading sharply with intrusion by malicious network nodes.

A layered architecture for security in [23] was designed providing for simplicity, modularity, flexibility and protocols standardization. The 5 layers-End to end security layer, routing security layer, network security layer, communication security layer and trust infrastructure layer were described. Yang et al [24] discusses a resiliency oriented security solution for security threats. It minimizes effect of malicious attacks and copes with network faults like extreme network overload, node misconfiguration, and operational failures.

Pirzada and McDonald [25] provided a protocol to implement security in AODV protocol ensuring protection of route discovery and data transfer. The scheme in [25] is dependent on point to point and end to end encryption using symmetric key based mechanism. Active and passive attacks are evaded by efficient key verification mechanism and multilayered enciphering.

3. METHODOLOGY:

This work observes the impact of malicious MANET nodes. DSR routing protocol is used. The work's goal was measuring and comparing the network performance variation due to maliciousness.

3.1 DSR Routing In MANET

DSR protocol is an on-demand routing protocol based on source routing. Mobile nodes have to maintain route caches with source routes of which the mobile is aware. Entries in route cache are updated as new routes are learned. The protocol has 2 major phases: route discovery and route maintenance. When a mobile node has to send a packet to a destination, it consults its route cache first to determine whether it already has a destination route [6]. If it has an unexpired destination route, it uses this to send the packet. But, if the node lacks such a route, it initiates route discovery by broadcasting a *route request* packet. This contains the destination address with the source node's address and a unique identification number. A node receiving the packet checks if it knows of a destination route. If it does not, it adds its address to the packet *route record* and forwards it on outgoing links. To limit route requests propagated on a node's outgoing links, the mobile forwards a route request if the same is not yet seen by the mobile and if mobile's address has not appeared in the route record.

A *route reply* is generated when route request reaches the destination or an intermediate node having an unexpired route to the destination [8] in its route cache. When the packet reaches the destination or an intermediate node, it has a route record with the sequence of hops taken. Figure 4a illustrates formation of route record as route request propagates throughout network. If a node generating route reply is destination, it places route record in the route request into route reply. If responding node is an intermediate node, it appends its cached route to route record and generates a route reply. To return route reply, the responding node should have a route to initiator. If so, it uses that. Otherwise, the node may reverse route in route record if symmetric links are supported. If they are not supported, the node may initiate its route discovery and piggyback route reply on a new route request. Figure 2, shows route reply transmission with associated route record back to source node.

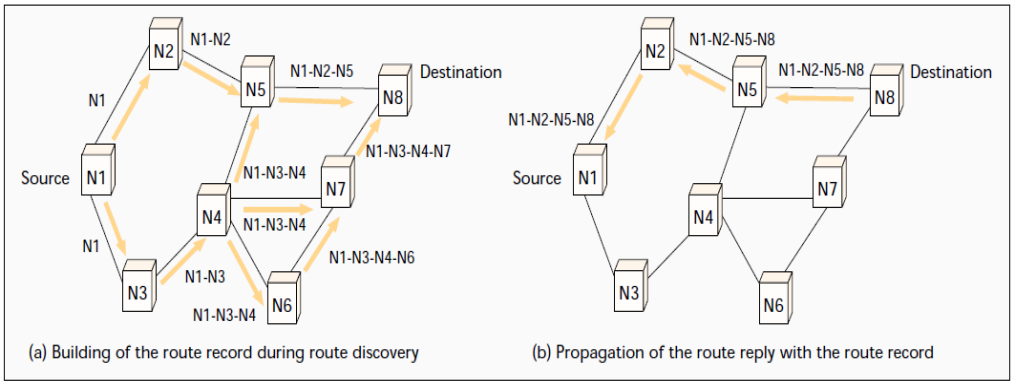

Figure 2 DSR route discovery process

Throughput

It is the ratio of total data that reaches a receiver from a sender to time taken for receiver to get last packet.

Average End-to-End delay

Average end-to-end delay is delay experienced by successfully delivered packets in reaching destinations. This is a good metric for protocol comparison denoting how efficient underlying routing algorithm is, as delay is based on optimality of path chosen. This includes delays caused by buffering during route discovery latency, retransmission delays at MAC, queuing at interface queue, and propagation and transfer times.

$$\text{Average End to End delay} = \frac{1}{s}\sum_{i=1}^{s}(ri - si).$$

4. RESULTS AND DISCUSSIONS

The experimental setup consists of 25 nodes distributed over two square kilometers. Three experiments are conducted the first network without malicious nodes and with 2% and 5% of the nodes being malicious.

4.1 Impact of Malicious nodes concentration on Throughput

Figure 3 show the impact of malicious nodes on throughput value. The following inferences can be drawn:

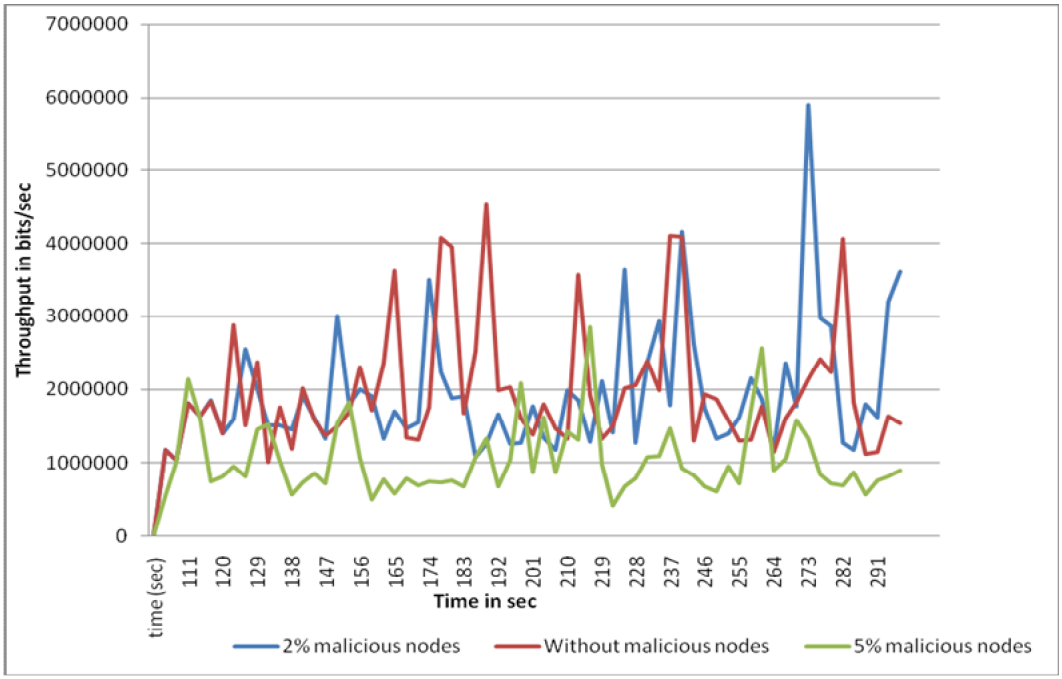

Figure 3 Throughput

The DSR routing protocol has highest throughput value when there is no malicious nodes. The results show a significant decrease in throughput due to malicious nodes and it is also seen that as the percentage of the maliciousness increases the negative impact is more. When the maliciousness is 2%, a drop of 2.17% in throughput is observed whereas when maliciousness is 5%, the throughput is 62.36% lower when compared to no malicious network.

4.2 Impact of Malicious nodes concentration on average end to end delay

Figure 4 shows the impact of malicious nodes on average end to end delay. The following inferences can be drawn: In general the end to end delay increases with the increase in malicious node concentration. When 5% of malicious node is present the delay is drastically higher by 74.74% when compared to network without malicious node.

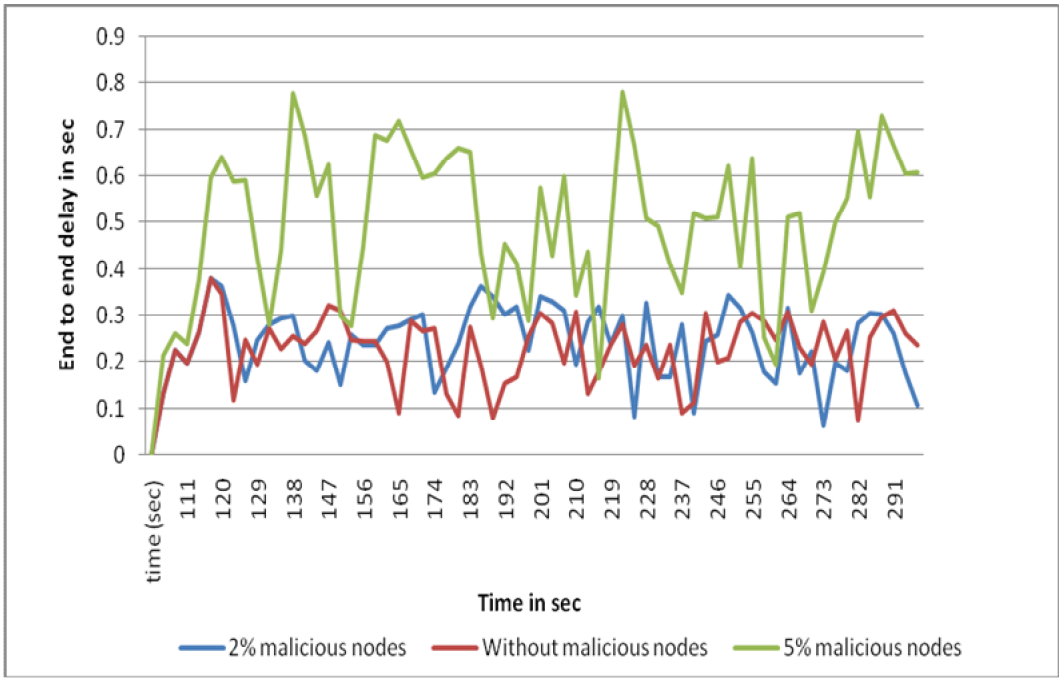

Figure 4 End to end delay

4.3 Impact of Malicious nodes concentration on Retransmission attempts in packets

Figure 5 shows the impact of malicious nodes on retransmission attempts. The retransmission attempts increases with the increase in maliciousness in the network.

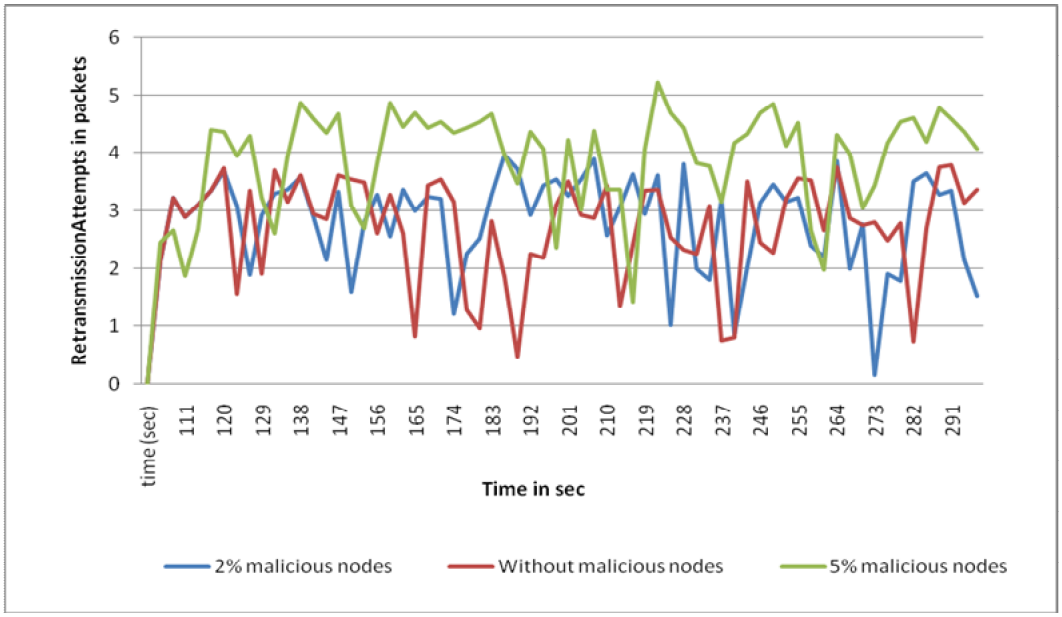

Figure 5 Retransmission Attempts

5. CONCLUSION

This paper makes an effort to find the impact of malicious nodes on DSR routing protocol performance. Experiments are conducted with 25 nodes distributed over two square kilometers. Three experiments are conducted; the first 2% of nodes are malicious, the second without malicious nodes and the third with 5% malicious nodes. The inimical and selfish nodes attacks, disrupts packet or do not forward the packet to the destination. Experimental results demonstrate that the network performance degrades sustainably due to maliciousness. It is also seen that as the percentage of maliciousness increase the performance degrades proportionally.

REFERENCE:

1. Asma Tuteja1, Rajneesh Gujral2 Sunil Thalia3, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2" NITTTR, Chandigarh, sunilthalia@rediffmail.com)

2. S. Ci et al., "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks," IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.

3. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato,Tohoku "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS" University Abbas Jamalipour, University Of Sydney.

4. Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati "Routing Security in Wireless Ad Hoc Networks"

5. Gowsiga, S. and Manavalasundaram, V. An Efficient and Secure Route Discovery for Mobile Ad Hoc Networks, Proceedings of the International Conference, Computational Systems and Communication Technology,2010.

6. David B. Johnson. Routing in ad hoc networks of mobile hosts. In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, pages 158–163, December 1994.

7. David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996.

8. E. Perkins and M. Royer, "Ad Hoc On Demand Distance Vector Routing", SuMicroSystem Laboratories Advance Development Group, Proceeding of the IEEE MOBICOM, pp 90-100, 1999.

9. Kravets, R., Naldurg, P. and Yi, S. Security-aware Ad Hoc Routing for Wireless Networks, In The ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC01), Long Beach, CA, 2001.

10. Hu, Y. and Perrig, A. A Survey of Secure Wireless Ad Hoc Routing, IEEE Security & Privacy, 28-39, 2004.

11. J.C. Kao and R. Marculescu, "Eavesdropping Minimization via Transmission Power Control in Ad Hoc Wireless Networks", Proc. IEEE Sensors and Ad hoc Communication and Networks SECON, 2006.

12. T. He, H. Wang and K.W. Lee, "Traffic analysis in anonyms MANETs", Proc. IEEE Military Communication Conference MILCOM, November 2008.

13. J. Kong, X. Hong and M. Gerla, "A new set of passive routing attacks in Mobile ad hoc networks", Proc. IEEE Military Communication Conference MILCOM, October 2003.

14. Batra, S., Goyal, P. and Singh, A. A Literature Review of Security Attack in Mobile Ad-hoc Networks, International Journal of Computer Applications, 11-15, 2010.

15. Haas, Z. and Zhou, L. Securing Ad Hoc Networks, IEEE Network Magazine, 24-30, 1999.

16. J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva", A Performance Comparison of Multi-Hop Wireless Network Routing Protocols," Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98), October 25-30, 1998, Dallas, Texas, USA, pp. 25-30.

17. S. R. Das, C. E. Perkins, and E. M. Royer, " Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks ", IEEE Personal Communications Magazine, Special Issue on Mobile Ad Hoc Networks, Vol. 8, No. 1, February 2001, pp. 16-29.

18. I Juan Jos´e Jaramillo, R. Srikan "A Game Theory Based Reputation Mechanism to Incentivize Cooperation in Wireless Ad Hoc Networks "t Coordinated Science Laboratory and Dept. of Electrical and Computer Engineering, University of Illinois, Urbana-Champaign, IL 61820, United States

19. " Ravilla, D. "Performance of secured zone routing protocol due to the effect of malicious nodes in MANETs Dept. of ECE, Manipal Univ., Manipal, India Putta, C.S.R. July 2013

20. Jain, S., Shastri, A. ; Chaurasia, B.K. "Analysis and Feasibility of Reactive Routing Protocols with Malicious Nodes in MANETs" April 2013

21. Geethu Bastian, Arun Soman "EFS: Enhanced FACES Protocol for Secure Routing In MANET",.

22. Suman Deswal and Sukhbir Singh, "Implementation of Routing Security Aspects in AODV" International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010

23. Shuyao Yu, Youkun Zhang, Chuck Song, Kai Chen “A security architecture for Mobile Ad Hoc networks”

24. Hao Yang, Haiyun Luo, Fanye, Songwu Lu, and Lixia Zhang “Security in mobile ad hoc networks challenges and solutions”

25. Pirzada and Chris McDonald “Secure routing with the AODV protocol” 2005 Asia-Pacific Conference on Communications, Perth, Western Australia, 3 - 5 October 2005.