Exploration of security threats and its performance impact on Mobile Ad-Hoc Networks using NS-2

S. C. Mandhata
Department of Computer Science & Engineering, DRIEMS
Cuttack-754022, India

S.N. Patro
Department of Computer Science & Engineering, DRIEMS
Cuttack-754022, India

S.P. Mohanty
Department of Mathematics, College of Engineering & Technology, Techno Campus,
Bhubaneswar-651003, India

ABSTRACT

In recent days Mobile Ad Hoc Network (MANet) has drawn the attention of many researchers largely owing to the inherent characteristics and varied applicability. Unlike traditional wired network, MANet has no clear line of defense. Moreover, the intrinsic properties of MANet expose many nontrivial security challenges. Security is of the prime concerns for network designers in any network. But for MANet, which allows both legitimate network users and malicious attackers to access the network, security issues have been a permanent concern because of the open shared wireless link and nomadic nature of nodes. We present a classification of MANet security threats based on protocol layers of network, security goals, behaviors, timings. Further, we perform a quantitative evaluation of impact of one of these attacks on an insecure on-demand routing protocol using simulation. Ad Hoc on-demand distance vector (AODV) routing protocol was chosen for the implementation of relative strength of the attack and is analyzed in terms of the magnitude of disruption per adversary.

Keywords

AODV, Attack, MANet, NS-2.x, Security

1. INTRODUCTION

MANet is a self organized network consisting of a collection of mobile nodes capable of communicating with each other without pre existing fixed communicating infrastructure. With the ability to establish network in any place at anytime, MANet facilitates the widespread adoption of mobile communicating devices combined with recent advancement in wireless technology which leads to increase in productivity in the corporate and industrial sectors by simplifying the complex business models. In the MANet, nodes can directly communicate with other nodes within their transmission ranges [1] whereas nodes that are not within the direct communication range use intermediate node(s) to communicate with each other which is referred to as multi-box communication. Each of the nodes act as both host and a router at the same time. Nodes arbitrarily change their positions resulting in a highly dynamic network topology causing wireless links to be broken and re-established on the fly [2].

The inherent characteristics of MANet[3] poses a number of non trivial challenges to security design. There is wide variety of attacks that targets the weakness of MANet. For example, routing control messages are important component of mobile network communication which is used in route discovery or route maintenance phase and malicious routing attack can target this by not following the specification of routing protocol. There are also attacks that target some particular routing protocol such as AODV & DSR. In this paper, an attempt is made to analyze the impact of such attack through simulation.

The remainder of this paper is organized as follows: in section 2, the vulnerability of MANet in terms of security challenges and security goals are discussed. Security threats are classified according to different perspective in section 3. Section 4 gives a brief discussion of the network simulator NS-2, modeling an attack, implementation and result analysis. Conclusion of the work and suggestion for future work is presented in section 5.

2. SECURITY CHALLENGES

MANet is an autonomous system of mobile nodes. Unlike fixed wired network in which the concept of network firewall is intended to provide an access control division between the insecure public network (the Internet) and the seemingly secure private network; there is no prevention of secure access mechanism. Assumption about physical security of MANet is unrealistic by the fact that wireless shared medium is completely exposed to outsiders and susceptible to attacks that could potentially target any of the layers of the networks. In addition to this other non-trivial challenges such as open peer-to-peer architecture, limited resource constraint, dynamic topology and lack of clear line of defense, insecure operational environment, lack of centralized management and scalability do exist.

Shared wireless medium: The wireless shared medium is completely exposed to outsiders and susceptible to attacks that could potentially target any of the layers in the network stack.

Dynamic topologies: Nodes are free to join, leave and move arbitrarily; thus, the network topology – which is typically multi hop and may change randomly and rapidly consisting of both bidirectional and unidirectional links. Nodes membership may disturb the trust relationship among the nodes. Resulting in Byzantine failures encountered in the routing protects for MANet [4].

Lack of secure boundaries: it is evident from the nature of MANet that it lacks clear line of defense because of the fact that node(s) can join, leave and move inside the network. Unlike fixed wired network in which adversary must get physical access to the network medium or even pass through the lines of defense in the form firewall or gateway before they can perform malicious behavior to the targets [5],

MANet is susceptible to varied link attacks which can come from any node that is the transmission range of any other nodes in the network.

Lack of centralized management: Absence of centralized management in MANet makes it difficult to identify whether the attack is caused by adversaries or because of benign failures. Monitoring the traffic of a highly dynamic large MANet is a difficult task and is even more difficult when adversaries frequently change their pattern and targets for attack. In MANet, all the nodes in the network are required to cooperate in network operations, while no security association can be assumed for all the network nodes. A clear line of operation between trusted and un-trusted nodes cannot be achieved by performing a priori classification resulting in impede of trust management for the nodes in the MANet [4]

Limited Resources: Battery power, bandwidth and computational power are scarce resources in MANet. Knowing the limited battery power adversary can send additional packets to the target continuously for routing or even can induce the target to be trapped in some kind of time-consuming computation resulting in denial of service. Limited battery power sometimes can be a cause for a node to behave in a selfish manner and refrain from usual assumption of cooperating with other nodes in network operations.

Bandwidth of wireless link will continue to have significantly lower capacity than their wired counterpart. The effect of the relatively low to moderate link capacities is congestion as aggregate application demand is likely approach or exceed link capacity frequently.

Scalability:
Scalability is an important issue concerning security vulnerabilities. Security mechanism should be capable of handling network that is continuously and dynamically changing. Routing protocols and key management services should be compatible to such a changing environment.

Security Criteria:
The key attributes to secure mobile ad hoc network are;

1. **Availability:** It ensures that the services offered by the node will be available to its users when it is expected i.e. survivability of network services despite denial of service attack.
2. **Integrity:** It guarantee the identity of message and ensures that message is never corrupted. Alteration of message during transmission can be either accidental or malicious.
3. **Confidentiality:** It ensures payload data and header information is never disclosed to unauthorized nodes.
4. **Authenticity:** It ensures the identity of peer nodes in communication. In the absence of authentication, an adversary can impersonate a trusted node and get access to the confidential resources or even propagate some fake message to disturb the normal network operations.
5. **Authorization:** It is used to assign different access rights to different level of users. In the process of authorization, credential is issued by certificate authority specifying the privileges and permissions which cannot be made false.
6. **Non-repudiation:** It ensures origin of a message cannot deny having sent the message. This is useful for the purpose of identifying whether a node with abnormal behavior is compromised or not. If a node recognizes that the message it has received is erroneous, it can then use that message as an evident to notify other nodes about the compromised node.
7. **Anonymity:** It protects the privacy of the nodes from arbitrary disclosure to any other entities. Information relating to the identity of owner or current user is kept private and not disclosed by the node.

3. CLASSIFICATION OF ATTACKS

Attacks in MANet can be classified in different ways. The attacks target different aspects of MANet environment and can be broadly classified into passive attack and active attacks. Categorization of attacks in MANet can be viewed differently in different context of discussion i.e. security goals, network topology, network functionality, users and applications classification of attacks can also be done for different layers of network. [2]

Passive attack: Passive attacks are those launched by adversaries to snoop the data being exchanged in the network. The attacker simply eavesdrops on network traffic so that traffic analysis can be done and user profile can be created. The requirement of confidentiality is breached if an attacker is able to interpret the information gathered from snooping. At the first sight these attack looks innocuous but can be mysterious when combined with active attacks. The network functionality do not get disrupted by such attacks and thus identification of such attacks becomes very difficult. The effect of such attack can greatly be reduced by employing some powerful encryption techniques. Passive attacks includes snooping, eavesdropping, traffic analysis and monitoring.

Active attack: Active attacks on the other hand attempts to modify, destroy information being exchanged in the network resulting disruption in normal network functionalities. Example of such attacks include modification of packets, routing information, replay of old packets, impersonating different identity or even in the form of denial of services resulting from extensive flooding of network and jamming of physical communication channel. Attacks can also be classified as internal attacks and external attacks. Internal attacks are launched by compromised node within the network. A compromised node tries to collect securities information and can access the protocol rights of the network. Since the compromised node which is earlier a legitimate and authorized node, it is very difficult to identify internal attacks. External attacks are launched by adversaries that do not belong to the network. Such attacks can be prevented by powerful encryption techniques and firewalls.

Goal based attacks: Security is the combination of process, procedures and systems to achieve its goals such as availability, confidentiality, authorization, integrity, non-repudiability etc. In the following figure attacks are classified according to the key attributes of security in MANet as shown in fig-1.

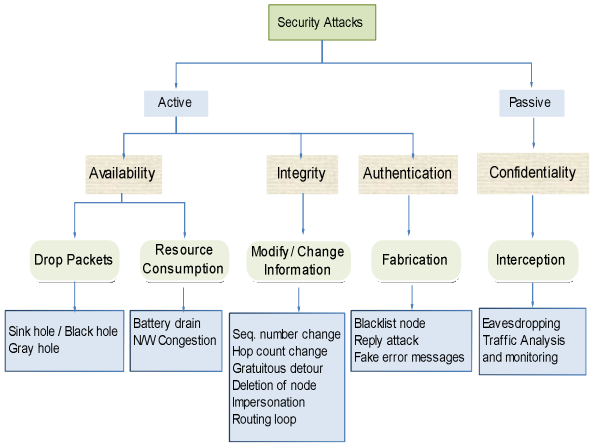

Fig-1: Security goal based classification.

Layer Based attacks: Attacks in mobile ad hoc network can be classified with respect to different layers present in MANet which is listed in the table-1.

Table–1: Types of attacks in MANet attributed to different layers

Layers in MANet	Nature / Type of attack
Application	Repudiation, Data corruption
Transport	Session hijacking, TCP/UDP SYN flooding
Network	Black hole, Gray hole4, worm hole, Byzantine, flooding, resource
Data Link	Traffic, Analyzer, monitoring disruption (MAC (201-11)
Physical	Jamming, interception, eavesdropping
Multi-layer	DoS, impersonation reply, man-in-middle

Behavioral based attack: Attacks in the MANet can also be classified into different groups depending upon the behavior that causes the state changes in the network [11]. Behavior of adversaries such as dropping all or selective packets, attracting all the traffic towards itself, forging network packets or initiate frequent packet to cause DoS and launching of specific attack of particular timing such as route discovery can be classified into different groups. It may be noted that an attack can be classified into more than one group as shown in the following fig-2.

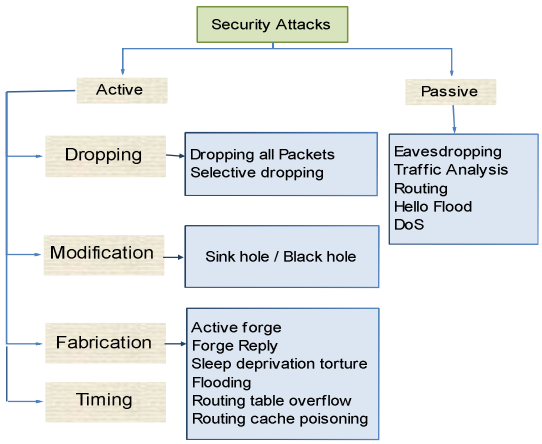

Fig-2 Behavioral based classification of attacks.

Cryptography based attack: Some of the security attacks can be combated by powerful mechanism of cryptography as weakness in security protocol lies in its poor implementation. Cryptographic primitives are considered to be secure [14] , however attacks such as collision attack on hash function e.g. SHA-1 [6], pseudo random number attacks [7], digital signature attack [8] and hash collision attacks [6]. The design and implementation of cryptographic pseudo random generators could be the cause of weakness to prevent replay attack.

Digital signature schemes such as RSA public key algorithm and DSA (Digital Signature Algorithm) suffer from various attacks. Hash collision attack aims at obtaining the hash that is same for two messages and could be used to tamper the existing certificate. While the key management protocols deal with the key generation, storage, distribution, updation, revocation and certificate service, lack of central trusted node in MANet makes more vulnerable in key management. In Fig-3 we have shown the classification attacks

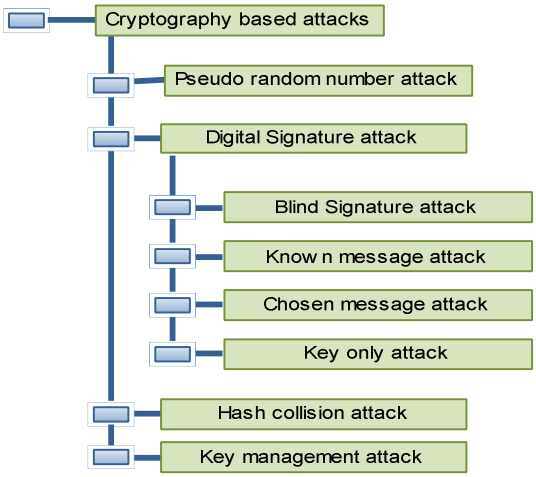

Fig-3 Cryptography based classification of attacks.

4. SIMULATION OF ATTACKS USING NS-2.X

4.1 The network simulator NS-2.x

NS-2 is a discrete event driven object oriented simulator which is used in research on networking. From among the wide variety of simulators available to the network researchers, NS-2 has been a popular one for its compatibility, extensibility and rich set of libraries that provide substantial support to the simulation of network features. NS-2 is based upon two languages; an extensible background engine implemented in C++ and the OTcl (the object oriented version of Tcl) used as the command and configuration interface. Each of these languages have their own class hierarchies; the C++ class hierarchy serves as the backend and termed as the compiled hierarchy while OTcl class hierarchy used as frontend and termed as interpreted hierarchy. Changes made during simulation through front end get reflected in the hierarchy through one to one correspondence [12] as shown in Fig-4. Tcl is the interface used to link between the two hierarchies.

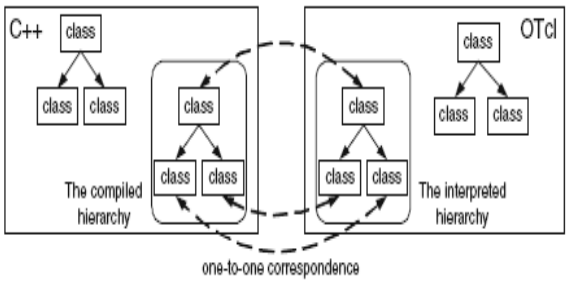

Fig-4: Independent & One-to-One correspondence in class hierarchies.

A simulation is defined by an OTcl script. Simulation of a specific configuration is done by setting up the desired parameters. A Tcl script used for simulation specifies;

- Definition of network topology (including the nodes, links, scheduling and routing protocols)
- Definition of traffic pattern (for example, the start and stop time of an UDP session, number of flows etc.)
- Definition of mobility scenario generation
- Collection of statistics and outputs the result of simulation into trace files.

From the users perspective, NS-2 is an OTcl interpreter that takes an OTcl script as input and produces a trace file as output from which analysis on performance metrics can be made [12] which is shown in fig-5.

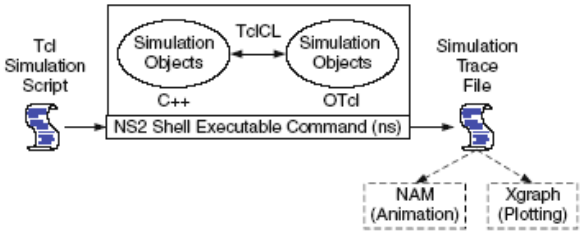

Fig-5: Users' perspective NS-2 simulation.

4.2 Modeling an attack in NS-2

As MANet is vulnerable to various attacks in different layers of protocol stack, modeling attack requires focusing a specific layer, designing and implementing the network components so that an analysis of performance metrics from the simulation result can be obtained. It has been a big challenge for a network layer routing protocol to function correctly and efficiently in the presence of malicious node which attempts to disrupt the routing service. Routing attacks can generally be characterized into routing, disruption and resource consumption by not forwarding the packets or adding and modifying some parameters of routing messages.

In this paper, we have made model of one attack and study the impact of malicious behavior of nodes present in the network with the assumption that the network is a broadcast network. The reactive protocol AODV is used as the packet forwarding protocol. An intermediate node drops all data packets to exhibit its malicious behavior and try to disrupt the network operation.

A node in NS-2 is a compound object which is composed of a node entry object and classifiers [13] as shown in Fig-6. NS-2 has an address classifier that does unicast routing and port classifier. A multicast node shown in Fig-7, in addition has a classifier that classify multicast packets from unicast packets and a multicast classifier that performs multicast routing.

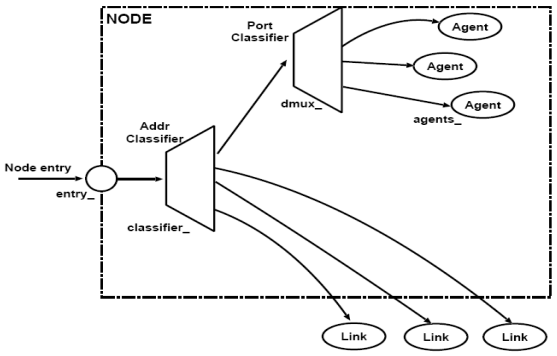

Fig-6: Internal Structure of a Unicast Node.

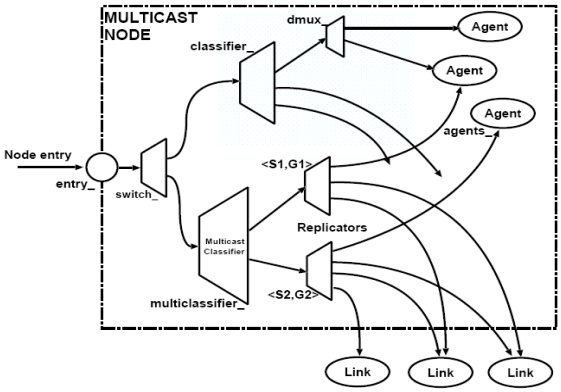

Fig-7: Internal Structure of a Multicast Node.

Unlike the real network packet, an NS-2 packet is composed of a stack of headers, and an optional pay load as shown in Fig-8. A packet header format is initialized when a simulator object is created where a stack of all registered headers such as common header that is commonly used by any objects as needed. IP header, TCP header, FTP header and trace header is defined and the offset of each header in the stack is recorded so that any network object can access any header in the stack of a packet using the corresponding offset value.

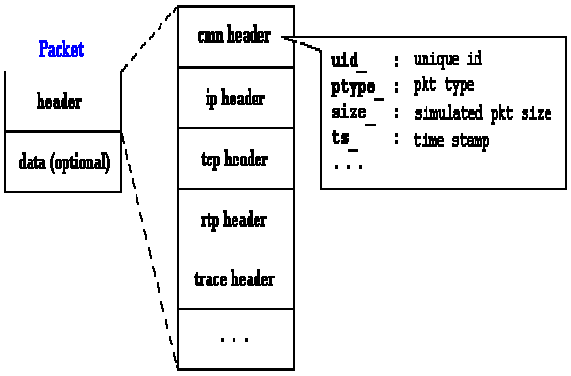

Fig-8: Structure of NS-2 Packet.

The packet header is analyzed by the classifier and forwarded to an outgoing interface which is the next downstream object in the network. The actual processing of the packet received by the node is done by the agent. An agent is a service or connection such as TCP/UDP with which two nodes in the network are connected. An agent's functionalities such as send, receive, forward and drop can be manipulated to launch an attack. Given below is the list of actions that are taken by a node agent upon receiving a packet;

- Extract the IP header of the packet to determine source and destination address.
- Extract the common header to determine packet type, size, next hop, previous hop etc.
- Extract protocol specific header of the packet e.g. RREP, RREQ, RERR etc.
- If the packet has already been received or has information that is older than it currently has or the packet has been generated by itself, then discard the packet by dropping.
- If the packet has latest information then forward the packet to the next hop if it has a route to the next hop.
- If the destination of the control packet is the node itself then generate a route reply packet and send it to the previous hop in the packet.

4.3 Implementation of attack in NS-2**:**

The attack discussed in this paper has been implemented in the network layer by modifying the existing code of AODV routing protocol [10]. Although the same attack could have been implemented by introducing new agent type into the simulator by taking scalability into consideration, our implementation also does not affect the normal routing functionalities of AODV in the presence or absence of a malicious node. In the presence of a malicious node in the network as an intermediate node, drops all data packets routed through it.

4.3.1 Simulation Parameters:

The configurable simulation parameters are shown in the Table-2. The experiments were carried out by introducing varying number of malicious nodes i.e. 0-5 in AODV routing protocol. The CBR traffic was used for the simulation with 5 flows.

Table–2: Configurable simulation parameters

Network Dimension	1500X1500m
Network size (# of nodes)	50
Radio range	250m
Mobility model	Random waypoint
Number of flows	5
Traffic type	CBR/UDP
Packet size	512B
Maximum rate of mobility	50m/sec
Number of malicious nodes	0-5

.

4.3.2 Addition / Modification of codes for the simulation

- Addition of codes in simulation script

```
#Setting nodes as hacker as per connection pattern
if {$par4==1} {
$ns_ at 0.0 "[$node_(11) set ragent_] hacker"}
if {$par4==2} {
$ns_ at 0.0 "[$node_(11) set ragent_] hacker"
$ns_ at 0.0 "[$node_(22) set ragent_] hacker"}
if {$par4==3} {
$ns_ at 0.0 "[$node_(11) set ragent_] hacker"
$ns_ at 0.0 "[$node_(22) set ragent_] hacker"
$ns_ at 0.0 "[$node_(26) set ragent_] hacker"}
if {$par4==4} {
$ns_ at 0.0 "[$node_(11) set ragent_] hacker"
$ns_ at 0.0 "[$node_(22) set ragent_] hacker"
$ns_ at 0.0 "[$node_(26) set ragent_] hacker"
$ns_ at 0.0 "[$node_(33) set ragent_] hacker"}
if {$par4==5} {
$ns_ at 0.0 "[$node_(11) set ragent_] hacker"
$ns_ at 0.0 "[$node_(22) set ragent_] hacker"
$ns_ at 0.0 "[$node_(26) set ragent_] hacker"
$ns_ at 0.0 "[$node_(33) set ragent_] hacker"
$ns_ at 0.0 "[$node_(36) set ragent_] hacker"}
```

- Modification of AODV code

The header file of AODV *aodv.h* contains the class definition and we add a Boolean variable as follows.

```
class AODV: public Agent {
...
bool            malicious;
...
};
```

The constructor of the class initializes the member variable to false as follows:

```
AODV::AODV(nsaddr_t id) : Agent(PT_AODV),
       btimer(this), htimer(this), ntimer(this),
       rtimer(this), lrtimer(this), rqueue() {
...
malicious=false;
...
}

AODV::command(int argc, const char*const* argv) {
...
//Setting the node as malicious if defined in Tcl as
'hacker'
   if(strcmp(argv[1], "hacker") == 0) {
     malicious = true;
     return TCL_OK;
   }
...
}

AODV::recv(Packet *p, Handler*) {
...
//     If I'm a malicious node
       if(malicious){
                drop(p,DROP_RTR_TTL);
                return;
       }
...
}
```

4.3.3 Result Analysis

The new trace format of NS-2 has been used which facilitates to obtain statics on number of performance metrics. Analysis on metrics such as packet drop is of our concern and packet delivery ratio is calculated accordingly. The results obtained

from the experiments is shown in the Fig-9 & Fig-10 and evident that as the number of malicious nodes inducted into the network are increased, the number of packets routed through these malicious nodes also increased significantly in comparison to the total number of packets sent.

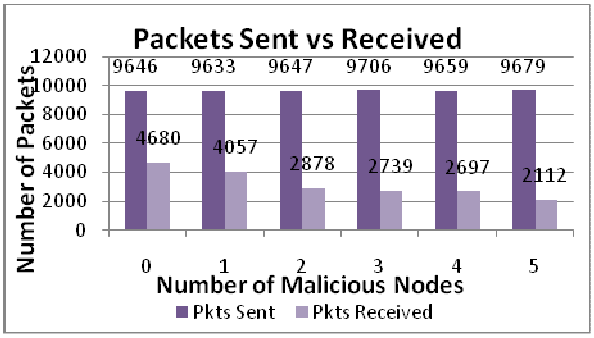

Fig-9: Number of packets sent and received in the Network having no malicious node and up to 5 malicious nodes.

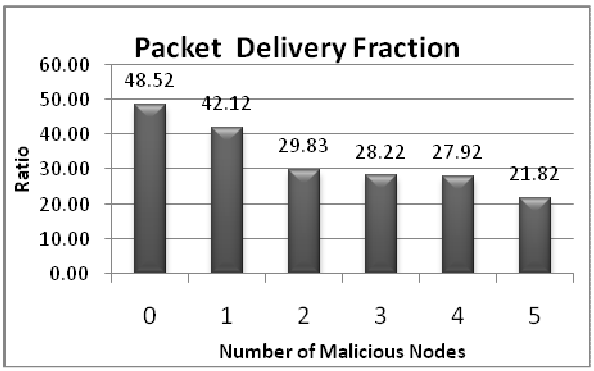

Fig-10: Packet Delivery Ratio of Network having no malicious node and up to 5 malicious nodes.

5. CONCLUSION.

In this paper, we studied various security threats and routing security issues in particular. One of these attacks was implemented and analysis of simulation result reveals that the performance metric such as packet delivery ratio is drastically affected as the existence of malicious nodes increased. As future work, we intend to carry out study relating to different intrusion detection mechanism and counter measures to such attacks and possibly devising a new or improved technique and implement the same. The performance should also be observed in a dynamic network configuration.

6. REFERENCES

[1] C. E. Perkins, "Ad Hoc Networks", Addison Wesley, 2001.

[2] C. Siva Ram Murthy & B. S Manoj, "Mobile Ad Hoc Networks - Architecture & Protocols", Pearson Education, New Delhi,2004.

[3] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and solutions", IEEE Wireless Communications, pp 38-47,2004.

[4] Amitabh Mishra and Ketan M. Nandkarni, in the Book, "The Handbook of Ad Hoc wireless Networks (Chapter-30)", CRC Press, LLC,2003.

[5] Yongguang Zhang and Wenke Lee, in the Book, "Ad Hoc Network Technologies and Protocols (Chapter-9)", Springer, 2005.

[6] X. Wang, D. Feng, X. Lai and H. Yu, "Collisions for Hash Functions MD4,MD5, HAVAL-128, and RIPMED", Cryptology ePrint Archive, Report 2004/199, http://eprint.iacr.org/, 2004.

[7] C.Kaufman, R. Perlman and M. Speciner, Network Security Private Communication in a Public World", Prentice Hall PTR, A division of Pearson Education, Inc., 2002.

[8] W. Mehuron, Digital Signature Standard (DSS), U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), FIPS PEB 186, 1994.

[9] D. Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4, 4th Quarter 2005.

[10] C. E. Perkins, S.R. Das, and E. Royer, "Ad-hoc on Demand Distance Vector (AODV)". March 2000, http://www.ietf.org/internal-drafts/draft-ietf-manet-aodv-05.txt

[11] Sevil Sen, John A. Clark, Juan A. Tapiador. "Security Threats in Mobile Ad Hoc Networks", Dept of Comp. Sc, University of York, YO10, UK

[12] T. Issariyakul, in Book "Introduction to Network Simulator NS2", Springer Science + Business Media, LLC,233 Springer City, New York NY 10013, USA, 2009.

[13] http ://www.isi.edu/nsnam/ns/ns-ducumentation. html.

[14] Bing Wu, Jianmin Chen, Ji Wu, Mihaela Cardei "A Survey of Attacks and Counter Measures in Mobile Ad Hoc Networks", Wireless / Mobile Network Security, Springer,2006.