Indian Journal of Science and Technology, *Vol 8(31), DOI: 10.17485/ijst/2015/v8i31/84085, November 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Biometric Identification System based on the Fusion of Palm print and Speech Signal

N. Priya*

Department of Computer Science and Engineering, Bharath University, Chennai - 600073, Tamil Nadu, India;
priya.cse@bharathuniv.ac.in

Abstract

Mobile Adhoc Network is an autonomous network formed by creating nodes and establishing wireless connections dynamically, so that messages in packets can be sent from a sender to receiver. The unique architecture of MANET offers several advantages and security challenges as passive and active attacks on the network. We discuss elaborately about the security attacks and two more popular security techniques, Intrusion Detection System (IDS) and Watchdog and Path rater (WPR). The two techniques are evaluated using two measures, viz., Availability Factor (AF) and Integrity Factor (IF). We present our results and our insights on suitability of a particular technique to a specific networking application. Our research is on-going and we indicate the extension possibilities that we are working upon.

Keywords: Availability and Integrity, Decentralized Management, Dynamic Routing, Intrusion Detection, Malicious Node, Prevention

1. Introduction

Mobile Adhoc Network (MANET) is popularly defined as a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. Unlike a wired network, nodes in an ad hoc network move freely, thus giving rise to frequent topology changes. MANETs can work independently or connected to the internet. The major advantages of MANETs are flexibility, mobility, infrastructure-less, and self-reconfiguration networks. However, MANETs are formed on a continuous basis, to enhance its features through designing new algorithms and protocols. The reconfiguration architecture and unique connection mechanisms in MANETs make it more vulnerable than the other wired and wireless networks.

2. Manet: An Overview

A mobile node in a MANET has two functions, *viz.*, as a host and a router. Communication of messages in packets is distributed among the nodes in a MANET; hence all nodes are co-operative and coordinating and there is no background network to control the operations. MANETs are formed in two layouts: single-hop and multi-hop. They differ in structure, implementation and the functionality cost. Formation of networks in MANET is a nonstop function of nodes and its topology and connectivity change quickly and continuously. These nodes can have access to a fixed infrastructure, as well. MANETs operate under different kinds of traffic that includes [1]: Peer-to-Peer when the communication occurs in one hop and steady traffic, Remote-to-Remote and stable route in a multi-hop network, so that level of traffic depends on the stability of the route and dynamic traffic where the connectivity is poor. Another feature of MANET is that (i) its links fluctuate in capacity, (ii) network bandwidth is smaller than in fixed networks' and (iii) links are less stable. A multiple session[2] can be conducted in one end-to-end route. Moreover, the terminals in MANETs are light-weighted, so the algorithms that helps in carrying out the functions of the mobile nodes in MANET should be very effective to suit their low capabilities.

**Author for correspondence*

3. Architectural Features

Infrastructure-less network: MANET connections are not established[3] using wired and wireless communication hardware, including Bluetooth technology. MANETs use satellites to create networks among nodes, which is an unusual method where the classical security solutions cannot be applied.

Limited power supply: One of MANETs features is that the nodes move freely within a network, and to facilitate that battery supply is employed; whereas wired networks operate using plugged-in electric power. This often creates a huge traffic of messages to avoid power supply run-out and denial of service. It further results in communication of unwanted messages and nodes turning selfish to decrease power consumption.

Limited physical security: The inherent dynamic connection mechanism in MANETs is a potential threat to physical security. Several kinds of attacks, such as denial of service and eavesdropping can be categorized under physical security[1].

Decentralized management: Decentralized management refers to the lack of a centralized server which overlooks and monitors the clients and connections. Due to the lack of a centralized control in MANETs, the level of difficulty of detecting attacks is very high. Intruders take advantage of benign failures and use various methods in attacking at different times, as connection mechanism is dynamic in a MANET. Further distinguishing trusted nodes from unsafe nodes is not easy considering the fact that MANETs are built using co-operation and coordination mechanisms.

4. Challenges and Barriers

Major challenges in MANETs are related to routing packets between two users especially in a multi-hop network, the proactive routing that MANET protocols follow[4] and the instability of multicast routing caused by a constant movement in the network. Security and reliability are some other key is-sues in MANET applications. A MANET faces many security challenges due to its low level of protection. Different kinds of authentication are required in a distributed MANET. Being a wireless communication protocol, consistency of service in MANETs is hard to achieve in instable environment. In addition, compatibility between infra-structured networks and MANETs is needed; also MANET operations consume a high power. The modules and algorithms and other aspects of MANETs need to be modified to reach a suitable level of efficiency. Many proposed protocols and projects are theoretically evident, but a majority of them fail to meet the requirements in actual applications.

4.1 Key Research Issues

The MANET network layer routing strategies present several issues; we discuss in brief four of these issues: X-cast routing, security & reliability, Quality of service, and internetworking mechanism.

X-cast Routing Algorithms: MANET should support each type of X-cast communication schemes. For example, multicast should tolerate the mobility of the nodes. Also multi-hop ad hoc network bring up more challenges because of the constant and random movement of the nodes, the routers and the non-malicious routes. Different traffic and mobility patterns resulted in continuous shifting between proactive and reactive schemes.

QoS Supporting Model: Quality of service function[5] is to pressurize data to different levels of connections. To maintain that, researchers have been studying a QoS module especially for MANETs to support multimedia and other applications in any environments.

Security, Reliability, and Availability Schemes: These three are most difficult to achieve in practice. Security protocols must be used to protect and secure the privacy of transferred packets and messages. There are similarities between the regular communication networks and MANETs in implementing confidentiality, integrity and availability. On the other hand, key management, authentication, and authorization are different because of the need of trusting a third party, which violates network security. Other problems that are characteristic of MANETs are interference, poor signals, low level error masking, recovery mechanisms, redundant routing paths, and how to increase routers' tolerance level, while balancing performance and reliability.

Internetworking mechanisms: Due to the difference of mobility of MANET nodes and the fixed networks, it is a huge challenge to achieve inter-operability between the two networks. One of the models that is been researched is a Mobile IP., where-in MANET nodes can communicate with other nodes in conventional networks and make itself reachable to these nodes, simultaneously.

5. Attacks in Manets

Two types of attacks target MANETs[6]; they are active and passive attacks. Active attacks are harmful and performed by malicious nodes that are destructive and have intrusive capabilities. On the other hand, passive attacks are done by selfish nodes that aim to preserve energy for themselves by not being involved in passing messages, which might result in partitioning the networks and decreasing the performance level of the networks. Each attack targets different part or layer of MANETs. Some examples of active and passive attacks are described in this section and Table I is a summary of active and passive attacks in a MANET.

5.1 Active Attacks

Black hole: Black hole is one of the most serious attacks on a network layer, where a malicious node declares by itself that it has the shortest valid route to the targeted destination. When an another node trusts this node, and sends a message or packet to the malicious node, it either changes the contents before forwarding it or just drops it.

Byzantine: Byzantine attacks affect the network layer because of a lack in authentication and packets integrity. These attacks are formed by a group of intermediate nodes that compromise their intentions within a network that results in deteriorating routing services of that network,

Table 1. A Summary of active and passive attacks on a MANET

Type	Name	Description	Target
	Denial of Service	Network bandwidth or resources are consumed by data floods triggered by malicious nodes	Data link layer
	Spoofing	Malicious nodes disguided as another, which give them advantages they don't deserve	N/A
	Black hole	Malicious nodes declare they have a right path for packets The packet in the route gets consumed and intercepted	Network layer
	Byzantine	Routine loops might be made, packets forded to bad routes or dropping packets by intermediate nods	Network layer
	Rushing	A wormhole is formed between two attackers then they rush route request packets to the nodes that receive the packet	Network layer
attacks	Partition	When fake routes are created by a malicious nodes to prevent nodes from communicating	Network layer
Active	Warmhole	Setting a shortcut by two or more malicious nodes that keep forwarding packets	Network layer
	Sybil attack	When a malicious node represents one of multiple identities	N/A
	Session Hijacking	Session hijacking happens because authentication happens only at the start of business	Transport layer
	Malicious Code	Operating system or user application gets attacked by viruses, Trojan horse, worms, spywares which damages network	Application layer
	Eavesdropping	Attacker aims to get confidential information during the communications	Physical layer
attacks	Interference	Attacker sends malicious data along with and jamming the same signals to be communicated	Physical layer
Passive	Traffic Analysis	Protocol engaging and provoked Communication between nodes	Data link layer

through dropping messages, forwarding them to invalid paths or creating routing loops.

Rushing: Rushing in MANET is an attack on network layer. Rushing causes mainly denial of services to nodes that uses on-demand ad hoc network routing protocols. The attack starts when a node initiates a ROUTE DISCOVERY to a targeted destination by forwarding a ROUTE REQUEST. For example, in figure 1, if the ROUTE REQUEST from the attacker is the first one that reaches the neighbors of the destination, then these neighbors will receive rushed REQUEST that was initiated by the attacker. Consequently, the neighbors will not be able to forward any other REQUEST other than the attacker, which, means that any REQUEST from the initiator will be discarded and denial of service will be a natural result of not finding valid routes to send the messages.

Partition: Partition is another attack on the network layer and is illustrated in Figure 2. Partition divides the network into two sets, by breaking one group of nodes from the other. In this attack, the malicious node aims to partition the network to prevent one group of nodes from contacting the other group, through injecting unreliable routing packets and make the route busy until the partition is completed.

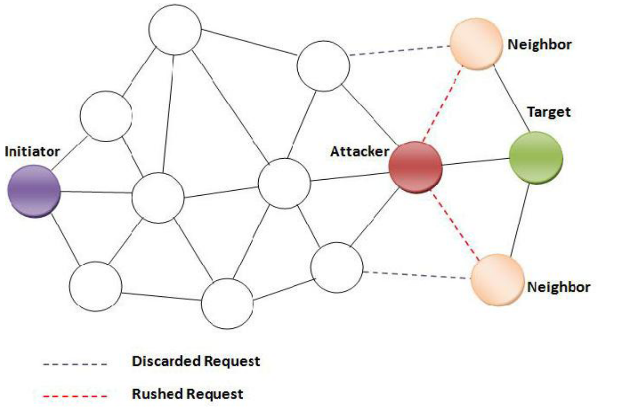


Figure 1. An illustration of Rushing attack.

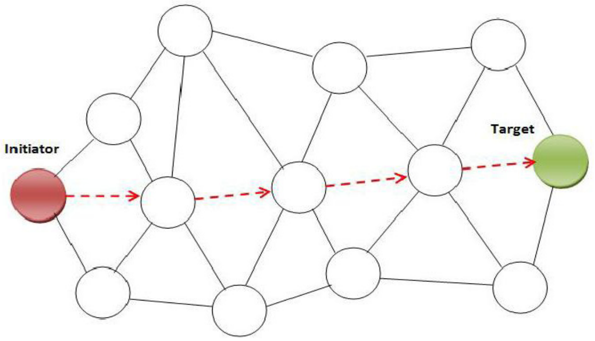


Figure 2. An illustration of Partition attack.

Wormhole: Wormhole attacks the network layer and an illustration is presented in Figure 3. [2] Wormhole attack or tunnel attack is where colliding malicious nodes create a tunnel or a short cut between them to be able to forward a packet to each other. These tunnels are extremely difficult to detect. Once they receive a packet in one end they send it through the tunnel to the other end and keep replaying it, which creates a great damage to the network.

Session hijacking: Session hijacking is an attack on the transport layer. In TCP or transmission control protocol an authentication happens only at the start of a session.

So the attacker takes the advantage of the absence of any authentication during the session and hijacks it to get an unauthorized access to confidential information.

Malicious code: Malicious code is an attack on the application layer. Malicious codes include viruses, spywares and worms that attackers use to achieve their goals in harming other nodes or getting access to confidential information. Such attacks have a negative impact on the network to slow down network and finally to damage it.

5.2 Passive Attacks

Eavesdropping: Eavesdropping happens on the physical layer. Nodes eavesdrop to obtain confidential information about other nodes such as passwords, public and private keys, which are denied under unauthorized access.

Interference and jamming: Interference and jamming at-tack the physical layer by sending signals that have the same frequency as the signals between a specific two nodes, to create many errors and random noise.

Traffic Analysis: Traffic analysis is an active attack on the data link layer, by provoking communication between nodes. Through this attack, the attacker obtains many

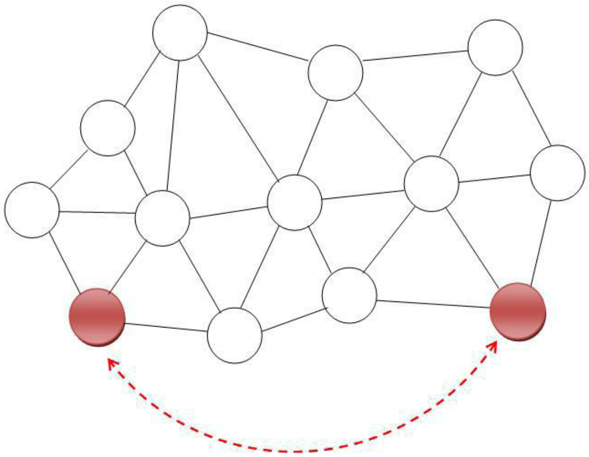


Figure 3. An illustration of Worm hole attack.

information about the network such as the location of the nodes and their roles, the topology of the network and the message routes.

6. Security Measures in Manets

We discuss five major measures of security in a MANET.

Availability: Availability in MANETs is making the re-sources of the network available[6] to other nodes regard-less of the attacks that target the network, especially denial of services or the existence of selfish nodes. Because communication in MANETs is based on cooperation and coordination, the ability to reach all other nodes in a network is imperative.

Confidentiality: Confidentiality is keeping certain information secret from other nodes that are not authorized to access that information. Certain information like pass-words or keys must have a defense mechanism to protect them and encryption is a more popular technique to achieve confidentiality.

Authorization: Authorization is a part of confidentiality to allow different credentials to different authorized nodes in a way that these credentials cannot be forged or falsified. For instance, to access secured information there should be a defense mechanism such as password protection. Anyone who does not know this password cannot access the information. Implementing different and newer methods of authorization would be useful to maintain the confidentially of sensitive information.

Integrity: Integrity refers to prevention of any compromises that may happen to packets when they are transmit-ted between nodes. Integrity offers little or no tolerance to any passive or active attacks that might target the packets. For instance, a packet cannot be dropped, altered or replaced by malicious code. Also a packet might not be attacked specifically by an intruder.

Authentication: Authentication is the ability to know the actual identity of other nodes[4]. Impersonating to gain access to secured information is made futile by authentication. A reliable authentication technique detects any impersonation and identifies all non-malicious nodes and messages, which is a fundamental security requirement.

7. Security Techniques

We discuss two effective techniques[3] in MANETs in this section. Intrusion detection technique is a security violation detection scheme and watch-dog/pathrater is a security violation prevention technique.

1) *Intrusion detection technique:* Intrusion detection Sys-tem or (IDS) is a system that detects any abnormality in the network. A small chip or an electronic piece is attached to all devices protected by IDS. This technique is also used in wired networks; however that differs from an IDS in MANETs[5]. This system can be applied on groups and individual nodes; however, it would be more efficient if it was implemented on a group of nodes.

In Figure 4, an IDS applied to a MANET is illustrated. Each node is capable of independent investigations, but they share and compare the information among them using an IDS agent implemented within each device, as mentioned before. Through this process, a node can obtain information about a wide range of the network, which will help in detecting any misbehaving in the

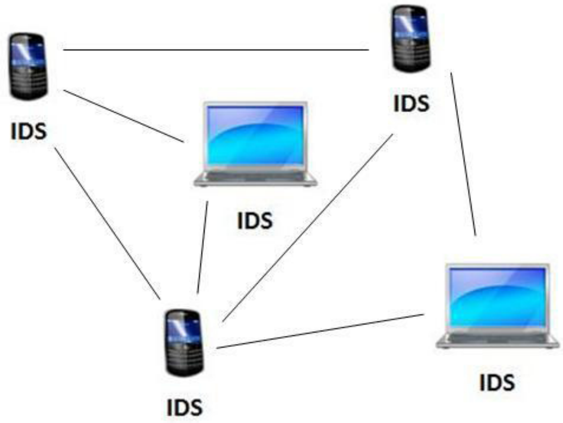
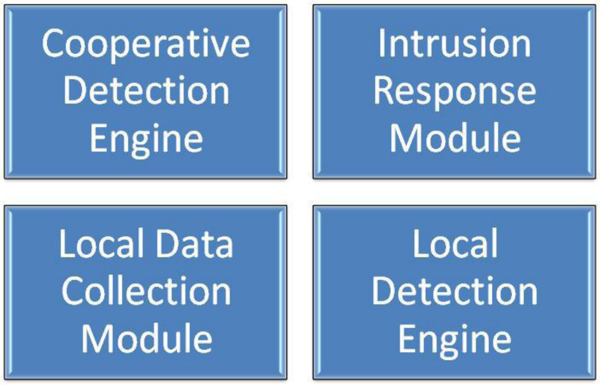


Figure 4. An Intrusion Detection system applied to a MANET.


Cooperative Detection Engine

Intrusion Response Module

Local Data Collection Module

Local Detection Engine

Figure 5. Internal Structure of an Intrusion Detection System

network, tracing it and dealing with it before any node is harmed[6].

Figure 5 represents the internal structure of an IDS system. An IDS [4] consists of four main modules. The first module is the local data collection module. This module is responsible of gathering the information of the network and the surrounding entities that exists around a certain nod in the system. The second module is the local detection engine that is responsible of analyzing the information that have collected by the local data collection module and recognizing any abnormality in the network[7]. This task can be done by observing the status of the network and report any suspicious changes. The third module is the cooperative detection engine, which become active when an abnormality is detected. It is responsible of sharing the information with the other nodes in the network, to compare this information and to identify the type of the intruder. Once the intruder type is detected, the fourth module, which is intrusion response module, acts to protect the node through different approaches depending on the type of the intrusion. This technique is effective in partially solving issues regarding decentralized management. However, IDS system consumes considerable power, which escalates threats due to limited power supply[8].

2) *Watchdog and path-rater:* Figure 6 illustrates a watchdog and path-rater operation[7] in a MANET. These two techniques work in tandem to achieve prevention of a security violation and thus to provide a secure routing. Basically watchdog identifies misbehavior and path-rater rates nodes according to their reliability. Watchdog copies a packet and forwards it to a buffer, and then it sends the original packet to a node. After that, it snoops and checks if the node modified the packet. If the packet forwarded without any modification, then the watchdog gets rid of the copy. In contrast, if the packet was modified, then the copy stays in the buffer for a certain time[9]. If the time is out, the node will be marked as a suspicious node and if that behavior was repeated for a certain number of times, then the node is marked as malicious. After all of that, the information that the watchdog finds out go to the path-rater. The path-rater evaluates all the nodes that are in the same network that the path-rater's user is in and keeps these rates updated according to their behavior. Then it chooses the best routes to use.

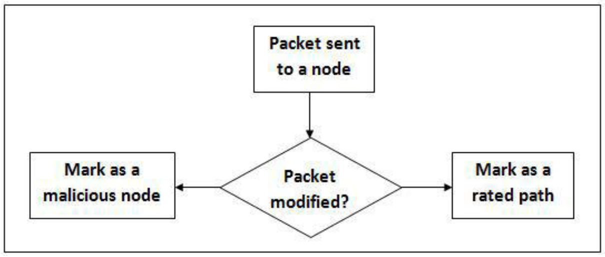


Figure 6. Illustration of watch dog and path rater actions.

8. Performance Evaluation

We have listed in detail about several passive and active attacks on MANETS and particularly two of the more popular security techniques in the previous section[10]. We simulated a Unicast MANET[8] using ns2 software. The simulation setting was an area of 2000m X 2000m and a random point way model with a node transmission range of 300 m were chosen. The experiments were repeated with two sets of 50 and 60 nodes and random partition attacks were induced using 0 to 10 malicious nodes in each set. We implemented algorithmic procedures for Intrusion detection system (IDS) and Watchdog and path rater (WPR) discussed in Section VII. Two security measures discussed in Section VI, viz., Availability and Integrity were used to evaluate the two security techniques. Availability factor (AF) and Integrity factor (IF) are the two proposed evaluation measures; *AF* is the ratio of the shortest distance between MANET sender and intended receiver to the actual distance between sender and intended receiver in MANET route. *IF* is the ratio of the number of error free packets in received message to the total number of packets in transmitted message.

8.1 Results and Discussion

We present a series of charts to display the Availability factor and Integrity factor in our simulation settings[12]. In the charts that follow, availability factor/integrity factor is plotted on the Y-axis against the number of nodes on X-axis. Figures 7 and 8 denote the availability factors of Security techniques (IDS and WPR), with 50 nodes and 60 nodes respectively. In both the cases, average performance of IDS in better than that of WPR for the number of attacks simulated.

Figures 9 and 10 are the plots of Integrity factors of the security techniques (IDS and WPR) for a total number of

50 and 60 nodes in the domain, respectively. We observe that there is no significant difference in numerical performance factor. A more precise observation leads to a finding that WPR has a better IF measure than IDS in the simulated sets of attacks[13].

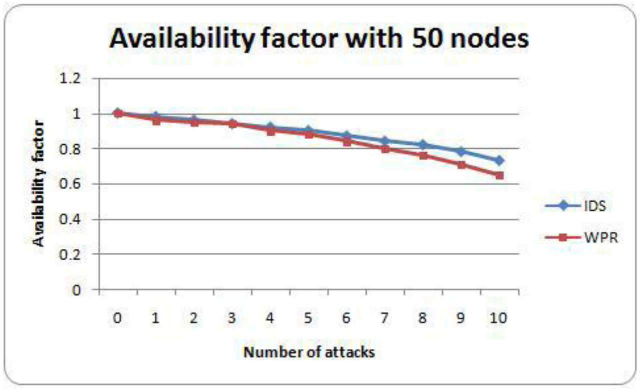


Figure 7. Availability factor against number of attacks with 50 nodes.

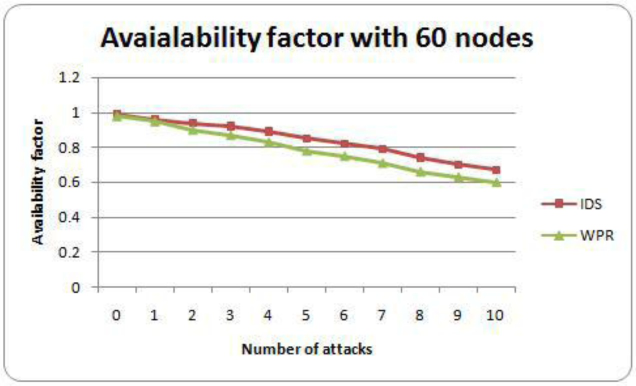


Figure 8. Availability factor against number of attacks with 60 nodes.

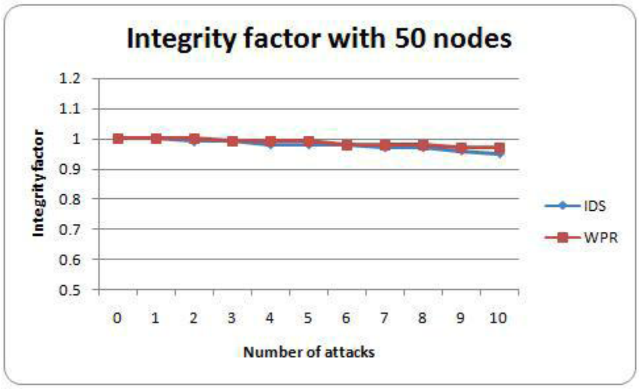


Figure 9. Integrity factor against number of attacks with 50 nodes.

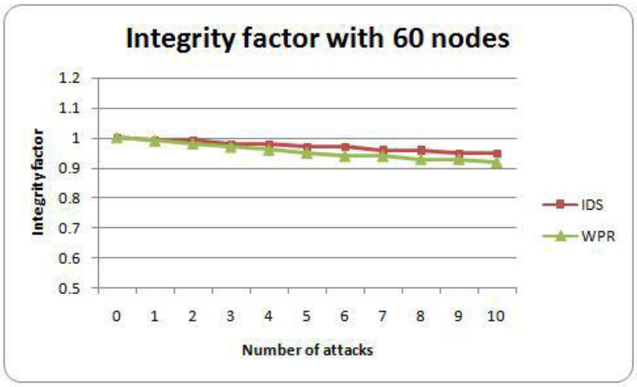


Figure 10. Integrity factor against number of attacks with 60 nodes.

9. Conclusion

We have discussed elaborately about several security attacks on MANETS, following brief discussions on the features, challenges in MANET implementation and some applications. Two more popular security detection and prevention techniques, namely Intrusion Detection system (IDS) and Watch-dog and Path rater (WPR) were considered for evaluations using two well defined security measures. The two measures that were considered were Availability factor and Integrity factor. The simulation setting and results were plotted and discussed. Availability measures of IDS is better than of WPR and Integrity measures of WPR is better than of IDS in our simulation study. We would interpret that our insights are interesting and beneficial to adopt a particular security technique that suits an application requirement. However this also leads to several questions to explore further. We have induced malicious attacks only by partition methods, whereas MANETS are prone to several other passive and active attacks, which we have discussed in details. Performance of security techniques to other types of attacks need to be further studied, which is our ongoing current work. We have also considered a Unicast MANET, whereas a multicast MANET is of equal practical relevance. These form some of our on-going research on MANETs.

10. References

1. Sun J-Z. Mobile ad hoc networking: An essential technology for pervasive computing. Proceedings of International Conferences on info-tech and Info-net. 2001. p. 316–21.
2. Kaliyamurthie KP, Parameswari D, Udayakumar R. QOS aware privacy preserving location monitoring in wireless

sensor network. Indian Journal of Science and Technology. 2013; 6(S5): 4648–52. ISSN: 0974-6846.

3. de Morais Cordeiro C, Agrawal D. Mobile ad hoc networking. Center for Distributed and Mobile Computing, ECECS, University of Cincinnati, 2002.
4. Sharmila D, Muthusamy P. Removal of heavy metal from industrial effluent using bio adsorbents (Camellia sinensis). Journal of Chemical and Pharmaceutical Research. 2013; 5(2):10–3. ISSN: 0975–7384.
5. Yu S, Zhang Y, Song C, Chen K. A security architecture for mobile ad hoc networks. 18th Asia-Pacific Advanced Network Meeting, Cairns, 2004.
6. Karlsson J. Rotuing security in mobile ad-hoc (manet) networks. International Research Seminar on Network Security and Next Generation Networks, Arcada University of Applied Sciences. 2009 Sep.
7. Udayakumar R, Khanaa V, Saravanan T, Saritha G. Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction. Middle - East Journal of Scientific Research. 2013; 16(12):1781–5. ISSN: 1990-9233.
8. Irshad A, Noshairwan W, Shafiq M, Khurram S, Irshad E, Usman M. Security enhancement in manet authentication by checking the crl status of servers. International Journal of Advanced Science and Technology. 2007; 91–98.
9. Jhaveri RH, Patel AD, Parmar JD, Shah BI. Manet routing protocols and wormhole attack against aodv. IJCSNS International Journal of Computer Science and Network Security. 2010 Apr; 10(4):12–8.
10. Kalaiselvi VS, Prabhu K, Ramesh M, Venkatesan V. The association of serum osteocalcin with the bone mineral density in post menopausal women. Journal of Clinical and Diagnostic Research. 2013; 7(5): 814–6. ISSN: 0973 – 709X.
11. Yang H, Luo H, Ye F, Lu S, Zhang L. Security in mobile ad-hoc networks: Challenges and solutions. IEEE Wireless Communications. 2004; 11(1):38–47.
12. Jayalakshmi T, Krishnamoorthy P, Kumar GR, Sivamani P. The microbiological quality of fruit containing soft drinks from Chennai. Journal of Chemical and Pharmaceutical Research. 2011; 3(6):626–30. ISSN: 0975–7384.
13. Available from: http://www.isi.edu/nsnam/ns/.