International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 3, April 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Secured Intrusion Protection System through EAACK in MANETS

Mr. Ravishankar Kandasamy[1], M. Ajith Kumar[2], M. Ajith Kumar[2], G. Arun Kumar[2]

[1]Assistant Professor, [2]UG Student,
[1,2]Department of Electronics and Communication Engineering,
[1,2]Paavai Engineering College, Namakkal, Tamil Nadu, India

ABSTRACT

Achieving reliable routing has always been a major issue in the design of communication networks, due to the absence of fixed infrastructure among which mobile ad hoc networks (MANETs) that can take control of the most adversarial networking environment, and the dynamic network topology the nature of open transmission media. In the MANETs these characteristics also more challenging to make the design of routing protocols. The network topology varies so to determining feasible routing paths for distributing messages in a decentralized is a difficult job. Factors such as the extensive distribution of nodes and open medium, variable wireless link quality topological changes, and propagation path loss become pertinent issues and make MANET unprotected to instructions. Thus, it becomes central to develop a systematic intrusion detection scheme to secure Mobile Ad Hoc networks from intruders. In this project, we put forward and applied an efficient IDS mechanism based on Enhanced Adaptive Acknowledgment (EAACK) especially made for MANETs which performs better than the earlier techniques such as AACK, TWOACK and Watchdog.

KEYWORDS: *Mobile Ad hoc Network (MANET), Acknowledgment (ACK), Network Simulator (NS2), Enhanced Adaptive Acknowledgement (EAACK), Misbehavior Report Authentication (MRA), Secure Acknowledgment (S-ACK), Digital Signature Algorithm (RSA)*

How to cite this paper: Mr. Ravishankar Kandasamy | M. Ajith Kumar | M. Ajith Kumar | G. Arun Kumar "Secured Intrusion Protection System through EAACK in MANETS" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-3, April 2020, pp.502-508, URL: www.ijtsrd.com/papers/ijtsrd30457.pdf

IJTSRD30457

1. INTRODUCTION

Wireless networking is the need of hour for many applications because of its easier network expansion, increased mobility improved responsiveness, better access to information, and enhanced guest access. In addition, with the increasing standard of industry and use of lightweight network hardware devices that is even smaller and largely mobile. The wireless communication is enhanced by Mobile ad hoc networks (MANETs) having high degree of node mobility.

Mobile Ad hoc Network (MANETs):

The Wireless cellular system is used in 1980s. The Wireless systems operate with the help of a centralized supporting structure access point. The adaptability of wireless systems limits the presence of a fixed supporting structure. Also known as, in there is no fixed infrastructure the technology cannot work effectively. The Future generation requires the wireless systems easy and quick. In the current system this quick network deployment is not possible. There will be a need for the rapid deployment of independent mobile users for the next generation of the wireless communication systems. Significant examples include establishing efficient, survivable, military networks, dynamic communication for emergency/rescue operations and disaster relief efforts. This network scenarios cannot depend on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. The Mobile ad-hoc networks networks operate in the absence of fixed infrastructure. It is not possible otherwise in they offer quick and easy network deployment in situations where. The Ad-hoc is a Latin word, it means "for this only." The each node in the mobile ad hoc network is connected by wireless links; every node operates as an end system.

Mobile Ad Hoc Network Applications

The Mobile ad-hoc network (MANET) can be used in crisis situations like military conflicts, emergency medical situation, natural disasters etc.

2. Literature Review

2.1. Detection And Prevention of Attacks on Manets Using Advanced Eaack And Hybrid Key Cryptography

In this paper we study different attacks on Mantes Such as Gray hole Attack Man in Middle attack, wormhole Attack, HTTP GET Food Attack. MANET having decentralized architecture in which all the node communicating in wireless manner. Thus, to increase the scalability of network there is need all node properly work together. MANETs are self-forming, self –maintained and Self-configuring allowing extreme network Scalability, & flexibility, which is often used in military conflict and medical emergency recovery. it oprets on single hop network and multihope network. Mantes is useful in emergency requirements where network range not possible and difficult to install network. Because it supports easy deployment, low cost, faster speed.

MANETS having distributed architecture therefore providing security to MANETS is very difficult**.** MANETs are an attractive technology used diplomatic and risky or planned applications due to facility provided by MANET's infrastructure. But MANETS moves from security issue. Security is measure problem because it not having central point control, it support dynamic topology, and it having wireless medium. Hence, it is crucial to develop an intrusion detection system in MANETs. In this paper, we aim to develop such an efficient and reliable intrusion detection system (IDS). Elliptic Curve Cryptography (ECC) algorithm is used to provide security to the data that is sent between the nodes. to reduce network overhead caused by digital signature Hybrid key cryptography technique is used. The disadvantage are ambiguous collision occur and receiver collision.

2.2. A Survey on Secure Intrusion Detection System for MANET

MANET (Mobile Ad hoc network) is an IEEE 802.11 framework which is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links. MANETs are self-forming, self maintained and self-healing allowing for extreme network flexibility, which is often used in critical mission applications like military conflict or emergency recovery. Unfortunately, the remote distribution and open medium of MANET makes them susceptible to various attacks. For example, due to lack of protection for nodes, malicious attackers can easily capture and compromise the mobile nodes to achieve attacks. Hence, it is crucial to develop an intrusion detection system in MANETs. In this paper, we aim to develop such an efficient and reliable intrusion detection system (IDS).

In this research paper, we have study a novel INTRUSION-DETECTION SYSTEM named EAACK protocol specially designed for MOBILE AD-HOC NETWORKs and compared it against other popular mechanisms in different scenarios through simulations. The demonstrated positive performances against Watchdog, TWOACK, and AACK. We also surveyed some intrusion detection systems that deals with various attacks. Attacker may find some new way to attack the system. Therefore system need to much robust so that it prevents new vulnerabilities and themselves. It is important to develop network security policies and deploy into MANET, this can be good research area. There should be system that learns from the knowledge of previous attacks and able to infer and detect new attacks; this can be potential research area. The drawback of this paper is limited transmission power.

2.3. Performance Enhancement of Intrusion Detection System Using Advance Adaptive EAACK for MANETs

A mobile ad hoc network (MANET) is a self-organizing and self-configuring multi-hop wireless network, where the nodes are free to move randomly. Ad hoc wireless network are self-creating and self-organizing. MANET solves this problem they allow intermediate node to transmit data between two other nodes. To achieve this by MANETs are divided into two types into two types of networks, namely, single-hop and multi-hop. Thus, all nodes are free to move randomly.

Considering the fact that MANET [1][2] is becoming popular among critical mission applications, network security is of most importance. Because of open medium and remote distribution of nodes in MANET they are vulnerable to various types of attacks. Moreover due to distributed nature of market centralized monitoring system is not feasible. In such case, it is crucial to develop an intrusion- detection system (IDS) specially designed for MANETs.

To detect misbehaving nodes with the presence of false misbehavior report and to authenticate whether the destination node has received the reported missing packet through a different route and to achieve this we have to focus on the comparative study of ACK, SACK & MRA scheme so the proposed protocol advance EAACK is compared against popular mechanism such as TWOACK,AACK and EAACK in different scenario through simulation. Simulation parameters that are considered in this paper is packet delivery ratio and delay. The results is positive performances against TWOACK, AACK and EAACK in the cases of link breakage and source maliciousness. The drawbacks are delay and link breakage.

2.4. An Improvised Intrusion Detection System for MANETs

MANET is a collection of mobile nodes. It is more popular these days MANET has a decentralized network infrastructure. Thus all nodes are free to move randomly. A centralized infrastructure, which is often infeasible in mission vital applications like military conflict or emergency recovery. Intrusion detection is the act of detecting surplus traffic on a network or a device. To detect unwanted activity and events such as illegal, traffic that violates security policy, and traffic that violates acceptable use policies. Attack prevention measures, such as validation and encryption, can be used as the first line of defence for reducing the possibilities of attacks. However, these techniques have a restriction on the effects of prevention techniques in general and they are designed for a set of known attacks. They attacks that are designed for circumventing the existing security measures. In this paper we are implementing the method of digital signature with multiple key generation schemes to enhance security by dividing the key into slots and sending it to the receiver

Mobile Ad Hoc Network has always been prone to securit**y** attacks. Since the existing methods concentrate only on

detecting the malicious nodes we are not aware of the validity of the acknowledgement packets on which we fully rely on. So to ensure to validate the acknowledgement packets we digitally sign the keys and transmit the keys. We also implement a method of generating multiple key by dividing keys into slots. This leads to maximum network security for the present scenario without the loss of network performance.

3. Proposed system

In traditional networks many intrusion detection systems have been proposed, the routers, gateways or switches are used for network traffic. Hence, it is easy to implement IDS in these networks. In MANETs we do not use such devices. Moreover, due to its openness so both malicious and legitimate users can access. In mobile environment it is very difficult to separate normal and unusual activities. Sometimes the false routing information can be generated by outdated node or from a malicious node due to the arbitrarily movement of nodes. Thus, the available intrusion detection techniques used in simple wired networks cannot be implemented to MANETs directly. Researchers have developed many intrusion detection systems for the MANETs. In the next section, we briefly explain three existing techniques, i.e. Watchdog, TWOACK, and (AACK).

3.1. ACK

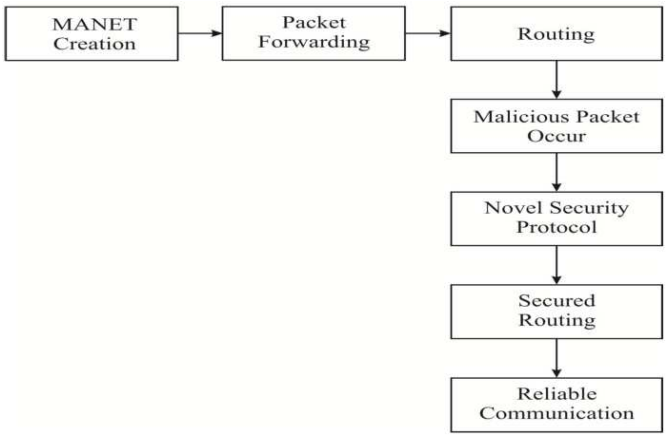
ACK is an end to end acknowledgment scheme. In EEACK It acts as a crossbreed scheme. The transmission from source to destination is successful when there is no misbehaving nodes. Then destination sends an acknowledgement packet to the source.

3.2. S-ACK

In the route the source sends S-ACK packet in the intention of detecting misbehaving nodes. After the packet reaches consecutive three nodes ahead the route the S-ACK sends the acknowledgement back to source. The third node is required to send the S-ACK acknowledgement to first node. S-ACK mode is the easy detection of misbehaving nodes in the limited power for transmission and the presence of receiver collision.

3.3. MRA

Misbehaviour Report Analysis (MRA) is a scheme. It is used to confirm misbehaviour report generated in S-ACK mode. This may be a false one as attacker may interfere in S-ACK scheme generating a false misbehaviour report.



Proposed Architecture

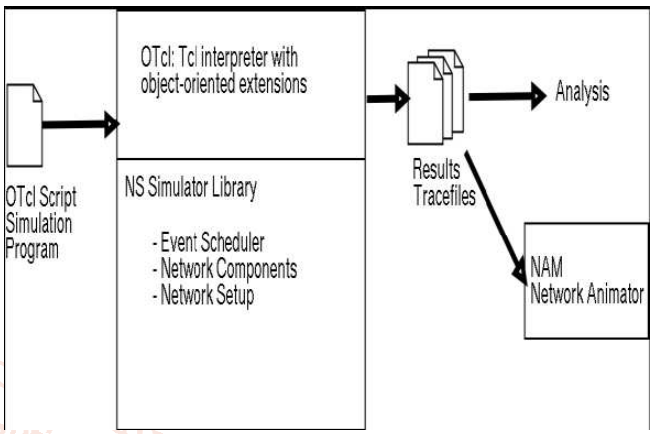
4. Explanation

4.1. The Network Simulator 2.33 (Ns2)

NS2 is developed at UC Berkeley it is a discrete event driven simulator. It is part of the VINT project. The objective of NS2 is to support networking research and education. NS2 is developed as a collaborative environment.

4.2. Structure of Ns2

Network simulator2 is built using object oriented methods in C++ and OTcl (object oriented variant of Tcl), NS2 interprets the simulation scripts written iOTcl.



Simplified User's View Of Ns

A subscriber has to set the different components up in the simulation environment. The user creates his simulation as a OTcl script. The event scheduler as the other component besides network components triggers the events of the simulation (e.g. sends packets, starts and stops tracing). Some parts of Network simulator2 are written in C++ for efficiency reasons.

4.3. Functionalities Of Ns2.33

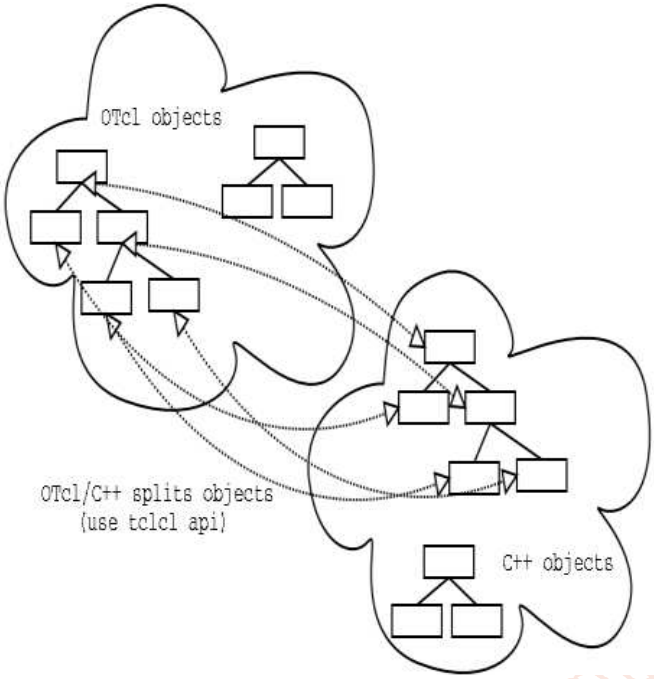
Functionalities for wired, wireless networks, tracing, and visualization are available in network simulator2.

➢ Support for the wired world include
- Routing DV, LS, and PIM-SM.
- Transport protocols: TCP and UDP for unicast.
- Traffic sources: web, ftp, telnet, cbr (constant bit rate), real audio.
- Different types of Queues: drop-tail, FQ, SFQ, DRR.
- Quality of Service: Integrated and Differentiated Services.
- Emulation.

➢ Support for the wireless world include
- Ad hoc routing with different protocols, e.g.
- AODV, DSR, DSDV, TORA
- Wired-cum-wireless networks
- Mobile IP
- Directed diffusion
- Satellite
- Senso-MAC
- Multiple propagation models (Free space, two-ray ground)
- Energy models

➢ Tracing
➢ Visualization
- Network Animator (NAM)
- Trace Graph

- Utilities
- Mobile Movement Generator



OTcl and C++: the duality

4.4. Mobile Networking In Ns2.33

This section describes the wireless model that was originally ported as CMU's(cracks me up) Monarch group's mobility extension to NS2. In this first section covers the original mobility model ported from CMU/Monarch group. Here we cover the internals of a mobile node, routing mechanisms and network components that are used to construct the network sk for a mobile node. The real CMU model allows simulation of pure wireless LANs or multihop ad-hoc networks.

4.5. The Basic Wireless Model In Ns

The wireless model fundamentally consists of the Mobile Node at the core, with additional supporting features that allows simulations of multi-hop ad-hoc networks.

The Mobile Node object is a split object. A major difference between them, though, is that the Mobile Node is not connected by means of Links to mobile nodes.

4.6. Mobile Node: Creating Wireless Topology

Mobile Node is the basic NS node object. It can be added with functionalities, ability to transmit and receive on a channel. It allows to be used wireless simulation environments, to create mobile.

Implementation Environment

NS2 can be used as the simulation tool. NS2 was chosen as the simulator partly because of the range of features it provides and partly because it has an open source code that can be modified and extended.

Network Simulator (Ns)

NS2 is an object–oriented, discrete event simulator for networking research. Even though the considerable confidence in NS, it is not a polished product yet and bugs are being finded and corrected continuously.

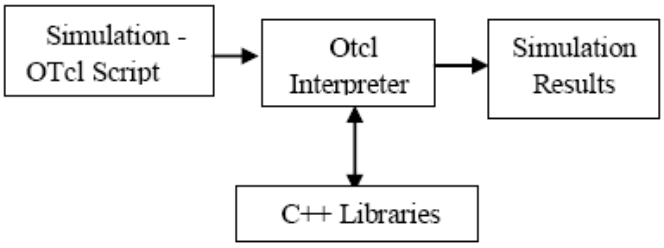
Network simulator2 is written in C++, with an OTcl1 interpreter as a command and configuration interface.

The C++ part, it is fast to run but slower to change, is used for detailed protocol implementation. One of the advantages of this split-language program approach is that it allows for fast generation of large events.

To simply use of simulator, it is sufficient to know OTcl NS can simulate the following:

1. **Topology:** Wired, wireless
2. **Scheduling Algorithms:** RED, Drop Tail,
3. **Transport Protocols:** TCP, UDP
4. **Routing:** Static and dynamic routing
5. **5.Application:** FTP, HTTP, Telnet, Traffic generators

4.7. User's View Of Ns-2



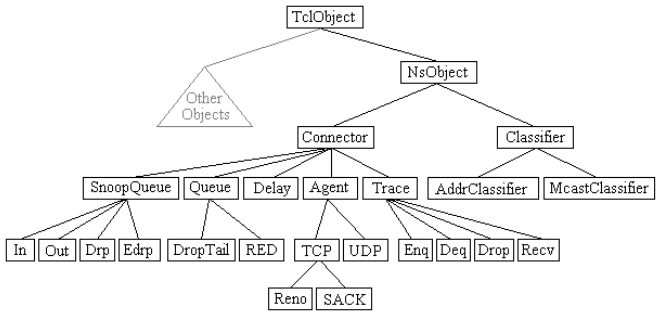
Block diagram of Architecture of NS-2

This section talks about the network simultor components, mostly compound network components. A partial OTcl class hierarchy of NS, which will used to help understanding the basic network components.

4.8. Class Tcl

The class Tcl (Telephone communication limited) encapsulates the actual instance of the OTcl interpreter and provides the methods to access and communicate with that interpreter, code. In this class provides methods for the following operations:

1. Obtain a reference to the Tel instance.
2. Invoke OTcl procedures through the interpret.
3. Store and lookup "Tcl Objects".



OTcl Class Hierarchy

4.8.1. Obtain a Reference to the class Tcl instance

A single instance of this class is declared in - tclcl/Tcl.cc as a static member variable.

4.8.2. Invoking OTcl Procedures

There are different methods to invoke an OTcl command through the instance, tcl.

1. **Passing Results to/from the Interpreter:** When the interpreter invokes a C++ scheme, it expects the result back in the private member variable, tcl-> result.

2. **Error Reporting and Exit:** In this method provides a uniform way to report errors in the compiled code.

4.9. Command Methods: Definition And Invocation

In every Tcl Object that is created, network simulator establishes the instance procedure, cmd{}, as a hook to executing methods through the compiled shadow object.

If there is no instance procedure called distance? the interpreter will invoke the instance procedure unknown{},it defined in the base class Tcl Object. The unknown procedure then invokes

$srmObject cmd distance? (agentAddre To show the operation through the compiled object's command()procedure. The user could explicitly invoke the operation directly.

For example,

```
        Agent/SRM/Adaptive instproc distance?
addr    {
        $self instvar distanceCache_($addr)
        if![info exists distanceCache_($addr)] {
        set distanceCache_($addr) [$self cmd distance? $addr]
        }
        set distanceCache_($addr)
        }
```

The following shows how the command() scheme using SRMAgent::command()

```
        Int ASRMAgent::command (int argc, const char*const*argv) {
        Tcl& tcl = Tcl::instance();
        if (argc == 3) {
        if (strcmp(argv[1], "distance?") == 0) {
        int sender = atoi(argv[2]);
        SRMinfo* sp = get_state(sender);
        tcl.tesultf("%f", sp->distance_);
        return TCL_OK; '
        }
        }
        return (SRMAgent::command(argc, argv));
```

The following observations are made from this code:
The function is called with two arguments. The argument (argc) indicates the number of arguments specified in the command line to the interpreter. The command line arguments vector (argv) consists of argv[0] contains the name of the method, "cmd" and argv[1] specifies the operation. In that this command method is defined for a class with multiple inheritance, one of two implementations can be chosen

1. Either they can invoke one of the parent's command method, and back to the result of that invocation.
2. They can each of the parent's command methods in some sequence, and back to the result of the first invocation that is successful. If none of them are successful, then they should back an error.

4.10. Mobile Networking In Ns

A major difference between them is that a mobile Node is not connected by means of Links to mobile nodes.

The common structure for defining a mobile node in ns2 is described as follows:

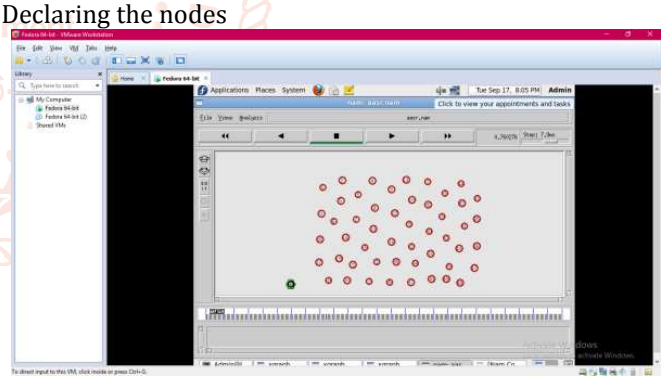
```
$ns node-config -adhocRouting $opt (adhocRouting)
        -IIType $opt (II)
        -macType $opt (mac)
        -ifqType $opt (ifq) -ifqLen $opt (ifqlen)
        -antType $opt (ant)
        -proplnstance [new $opt (prop) -phyType $opt (netif)
        -channel [new $opt (chan)]
        -topolnstance $topo
        -wiredRouting OFF
        -agentTrace ON
        -routerTrace OFF
        -macTrace OFF
```

The above API (application program interface) configures for a mobile node with all the given values of ad hoc-routing protocol, network stack, topography, propagation model, with wired routing turned on or off (required for wired-cum-wireless) and tracing turned on or off at different levels (router, mac, agent).

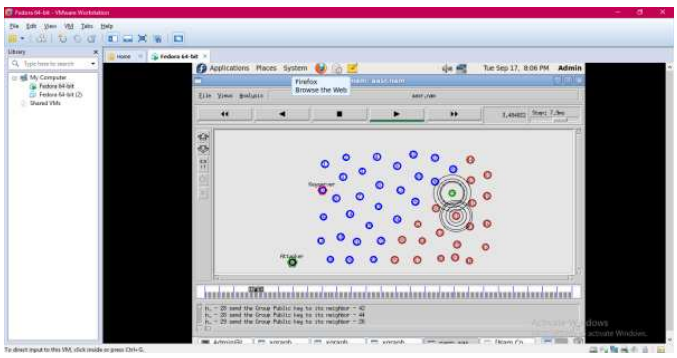
5. Result:

The simulation is conducted is with the Network Simulator (NS). The system is running on laptop with core 2 Duo t7250 CPU and 3GB RAM. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20m/s

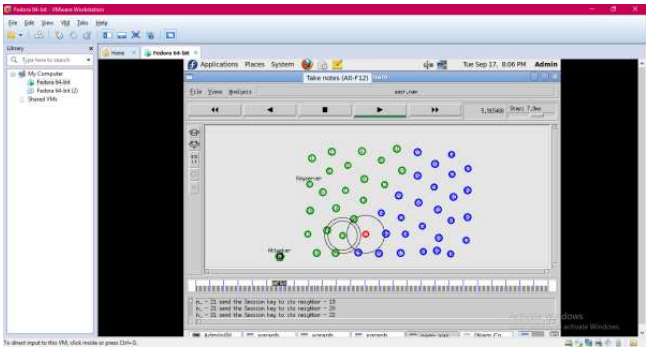
Declaring the nodes



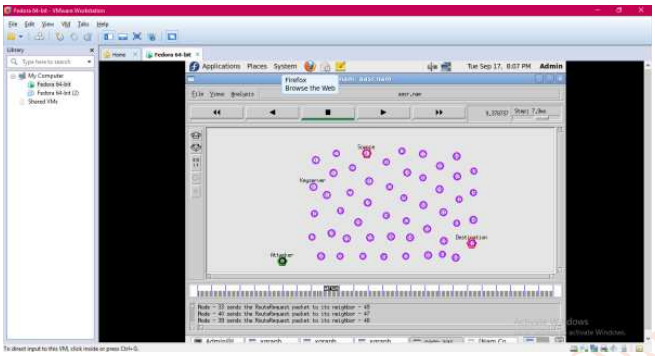
Broadcasting for finding the route for packet transmission.



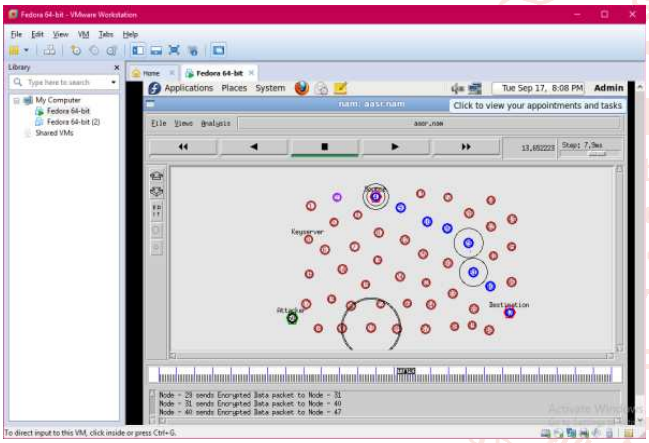
A path is chosen from source to destination.



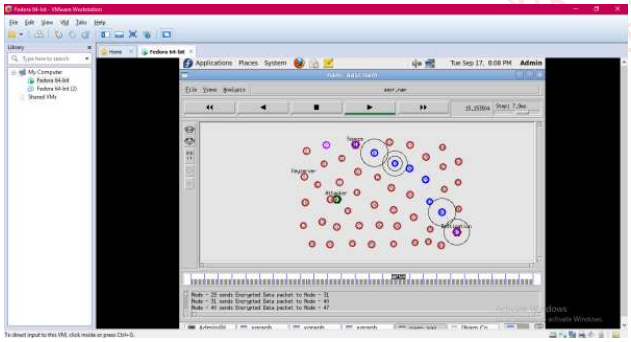
Declaring the source and destination nodes



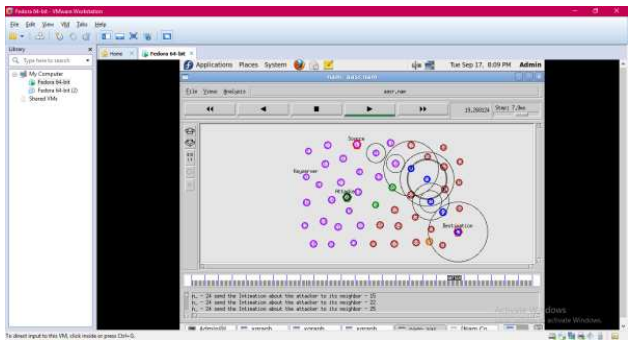
Searching the alternative path



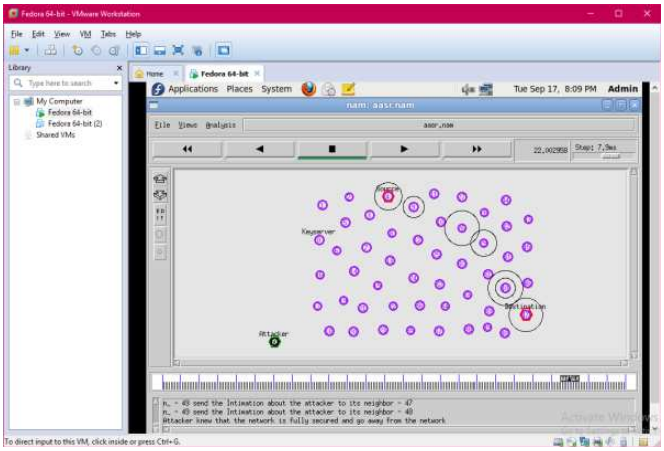
An alternative path is found.



The attacker nodes are detected in the current path so searching for an alternative path without malicious.



The message was sent.



The implementation of the system to detect malicious attackers in MANETs is done and the message was sent without any attacks.

6. Conclusion:

To solve the security issue in MANETS we implemented new IDS based on enhanced adaptive Acknowledgment (EAACK). In this method every acknowledgment packet is digitally signed before sending in network and accepted only after verification. The limited transmission power and false misbehavior of nodes are completely removed in this scheme. Every acknowledgment packet received are authentic and untainted. This reduces the need for costly secure routing behaviors designed to mitigate the effects of an untrusted environment (and untrusted nodes) on the routing process. By preventing the entry of potentially untrustworthy nodes to the network, and thus the routing process, a MANET may be protected from subversion of its routing services at a lower cost, as malicious nodes are barred from the process entirely. This provides security to all data communicated over a MANET. It specifically targets the attributes of MANETs, it is not suitable for use in other types of network at this time. It sacrifices adaptability to a range of networks, to ensure that MANET communication is completely and efficiently protected. A single efficient method protects routing and application data, ensuring that the MANET provides reliable, confidential and trustworthy communication to all legitimate node.

In real time environment this project can be extended further for many applications . To improving the encryption technique further studies is needed. it is time consuming process for reconstructing the message, which can be reduced further. The optimized routing techniques can be incorporated the finding shortest path.

REFERENCES

[1] A. Mishra, K. Nadkarni, and A. Patcha, \Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.

[2] A. Singh, M. Maheshwari, and N. Kumar, “Security and trust management in MANET,” in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[3] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, “Modeling and optimization of a solar energy harvester system for self-powered wireless sensor

networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[4] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5.

[5] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[6] K.Liu, J. Deng, P. K. Varshney, And K. Balakrishnan, "An Acknowledgment Based Approach For The Detection Of Routing Misbehaviour In Manets," Ieee Trans. Mobile Comput., Vol. 6, No. 5, Pp. 536–550, May 2007.

[7] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488-494.

[8] T. Anantvalee And J. Wu, "A Survey On Intrusion Detection In Mobile Ad Hoc Networks," In Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[9] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct.2009.

[10] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3-13.