International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 3 Issue 9, September – 2019, Pages: 26-30

Integrated Security for Mobile Ad-hoc Network

Hossain S.M.E[1], Mourad H[1], Arockiasamy S[1], Islam R[2], Yaqoob R[1]

School of Information Systems, University of Nizwa, Oman [1]
Department of ECE, Khulna University of Engineering & Technology, Bangladesh [2]
emdad.hossain@unizwa.edu.om

Abstract: *In this paper we are going to find out threats against Mobile ad-hoc networks (MANet) and find out possible solution(s) for those. As we are aware, the security threat is increasing as it has no fixed infrastructure, dynamic change in topology and limited bandwidth. Our aim is to propose an improved framework for general threats on MANet. This framework will provide better security in dealing with threats like hacking, threat in money transfer issues, leakage of confidential information.*

Keywords: MANet, Hacking, Threat, Confidential

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are an emerging type of wireless networking, in which mobile nodes associate on an extemporaneous or ad hoc basis. MANETs are both self-forming and self-healing, enabling peer-level communications between mobile nodes without reliance on centralized resources or fixed infrastructure [1]. However, there are some important metrics in MANET security that are important in all security approaches; we call them “Security Parameters”. Being unaware of these parameters may cause a security approach useless in MANET. Each security approach must be aware of security parameters. All mechanisms proposed for security aspects, must be aware of the parameters those we are going to explain in this paper and will not disregard them, otherwise they may be useless in MANET [2]. By considering the weakness of current security and importance of advanced security; in this paper we are proposing an integrated secure framework (simulators) for mobile ad-hoc network which will work like secure pipe-line on any communication. In fact we are going to use three different simulators for our experiment that are NS-2 (Berkeley’s Network Simulator), Omnet++, SANS **(**Simple Ad Hoc Network Simulator).

2. BACKGROUND

Security incidents can have severe consequences for mobile operators. Short-term public relations hiccups can be dealt with, but over the long-term, carriers are subject to subscriber churn, which can significantly influence profitability [3]. By extracting the importance, the Governments are getting involved, mandating that carriers abide by security legislation specially intended for telecommunication service providers. In the European Union, EU directive 2009/140/EC, article 13a, requires operators to take steps to provide uninterrupted and secure transmission of voice and data over EU telecommunications infrastructure. Operators are also required to report security incidents so the effectiveness of their controls can be measured [3]. Further, consisting of devices that are autonomously self-organizing in networks, ad hoc networks offer a large degree of freedom at a lower cost than other networking solutions. A MANET is an autonomous collection of mobile users that communicate over relatively “slow” wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. The primary goal of such an ad-hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner [4]. Existing key management mechanisms are usually based on central points where services such as certification authorities or key servers can be placed. Since MANETs do not have such points, new key management mechanisms have had to be developed to fulfill requirements. Since prevention techniques are invariably limited in effectiveness, intrusion detection systems are generally used to complement other security mechanisms. This applies to MANETs too and researchers have proposed new IDSs to detect malicious activities on these networks [5]. Furthermore, MANET has no fixed access points while every node could be router or host. MANETs lack prior organization and central administration, so security issues are different and thus require different security mechanisms. Wireless links in MANETs make it more prone to the attacks for attackers. Attackers can directly attack the internet to delete messages, add malicious messages [6]. Conversely, there are several security criteria to secure the important information. These are as follows:

1. Confidentiality
2. Availability
3. Integrity
   a. Malicious altering
   b. Accidental altering
4. Authentication
5. Authorization

6. Non-repudiation
7. Attacks using fabrication.

However, up-to-date researchers consider most advanced framework is 3D-Secure Framework designed for issuers to provide payment verification and authentication for Card-Not-Present (CNP) transactions [7]. Further, it can be applied to general mobile network security too. 3-D means (in the prospect) three (3) different layers of security. Perhaps, each extra security field added; it can seriously lower the number of completed transactions. Moreover some users might not know what 3-D Secure is and they can close the browser too. This of course will lead to lost sales/review for the mobile operator. We must also remember that there is an extra fee for the service [8]. Hence, mobile operator organization must take responsibility to educate their users on their own responsibility. Further, by considering benefit of our proposed 3-D security, we must ignore those minor drawbacks which are not even threats. Next section we are going to explain the methodology followed by experimental analysis of our adoption extensively.

3. METHODOLOGY

We are going to use three (3) different types of security framework which will provide three (3) dimensional (3D) results or three (3) dimensional protections towards our mobile network. Our proposed models are as follows:

Network Simulator 2 (NS2): NS is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. NS began as a variant of the REAL network simulator in 1989 and has evolved substantially over the past few years. In 1995 ns development was supported by DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. Currently ns development is support through DARPA with SAMAN and through NSF with CONSER, both in collaboration with other researchers including ACIRI [9]. There are number of noble reason to choose NS-2 for mobile ad-hoc network; that are:

- Improve flexibility.
- Provide access to information.
- Central Administration.
- Services regardless of geographic position.
- Robust Free Network.
- Networks can set up at any place and time.
- Easy Network set up.
- Independence from central network administration.
- Quick Integration [10].

Omnet++: OMNeT++ itself is not a simulator of anything concrete, but rather provides infrastructure and tools for *writing* simulations. One of the fundamental ingredients of this infrastructure is component architecture for simulation models. Models are assembled from reusable components termed *modules*. Well-written modules are truly reusable, and can be combined in various ways like LEGO blocks [11]. However, OMNeT++ is simulation tool which uses C/C++ as the frontend code and the Network Descriptor which is utilized to create the topography of the network. This tool also consists of header file (.h), initialization file (.ini) and cc file for writing the C++ code. The topography is designed in the NED file and the C++ code is written in the .cc file in which the headers are included from the .h file and are interlinked with .ini files. While running the simulation of topography the event window will be tracked down parallel in OMNeT++ tool. The efficiency of the network topography can be analyzed using the data retrieve while simulation. In this way the variations in the efficiency of the network topography can be studied and analyzed [12]. However, SANS (A Simple Ad Hoc Network Simulator) generally effective for the development and presentation of algorithms at the network and transport layer. We are going to discuss SANS on mobile ad-hoc network in next section along with an experimental analysis.

4. EXPERIMENTS and ANALYSIS

In the experiment section we are going to show number of extensive results with our stated methods above.

4.1 NS-2: We are going to use the Berkeley's Network Simulator (ns-2), for simulation routing protocols. It has in fact a good simulation environment which will cover the layout analysis for the security prospect. Further, the analysis could be done form the outputs too. The general process of creating a simulation can be divided into several steps like:

The network stack for a mobile-node consists of a link layer (LL), an ARP module connected to LL, an interface priority queue(IFq), a mac layer(MAC), a network interface(netIF), all connected to the channel. These network components are created and plumbed together in OTcl. The above procedure creates a mobile-node (split) object, creates an adhoc-routing routing agent as specified, creates the network stack consisting of a link layer, interface queue, mac layer, and a network interface with an antenna, uses the defined propagation model, interconnects these components and connects the stack to the channel. In this case the mobile-node now looks like the schematic which is clearly shown in Figure 1 below.

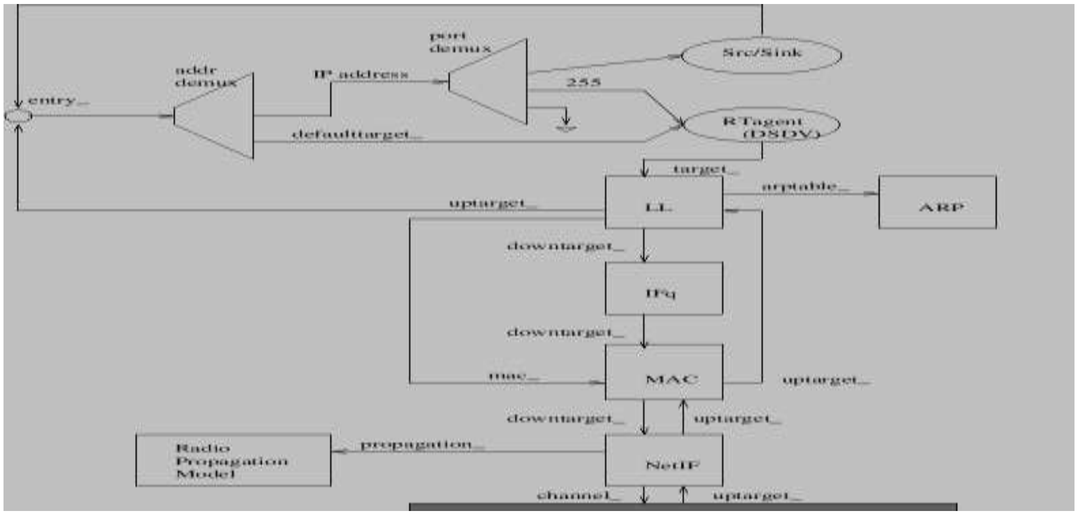


Figure 1: Schematic mobile-node [14]

The experimental result shows The mobile node structure used for DSR routing is slightly different from the mobile-node described above. The class SRNode is derived from class MobileNode. SRNode doesnot use address demux or classifiers and all packets received by the node are handed down to the DSR routing agent by default. The DSR routing agent either receives packets for itself by handing it over to the port dmux or forwards packets as per source routes or sends out route requests and route replies for fresh packets [14], which is one vital aspect to consider NS-2 for mobile ad-hoc network security.

4.2 Omnet++: It is an open source, component based simulation built on C++ foundation. It is a simulation framework. It performs simulation and performance analysis with the help of computer networks and network protocols.

- Each node in the network communicates with other node using radio waves.
- Due to the non-static nature, ad hoc network avoid the single point of failure and make the network more robustness.
- An ad hoc network is local area network that builds an automatic connection to the nodes in the network.
- The entire network is distributed and nodes are collaborated with each other without fixed station access point (AP) or base station.
- Due to the absence of centralized structure, the nodes in the ad hoc network acts as router to send and receive the data

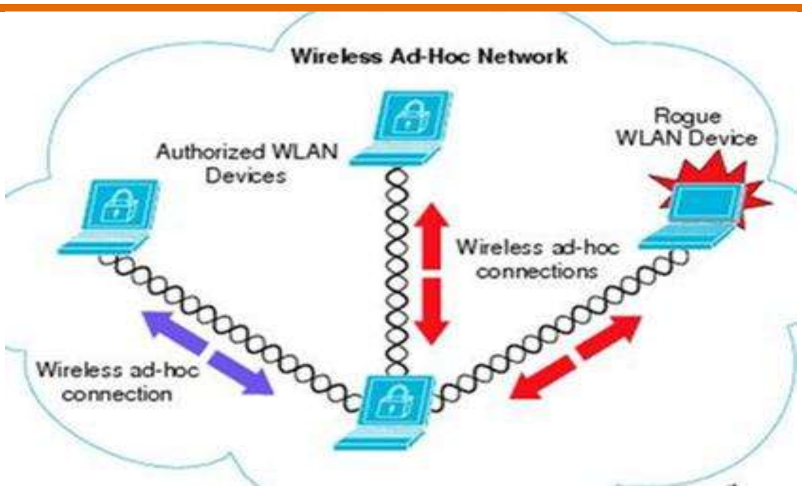
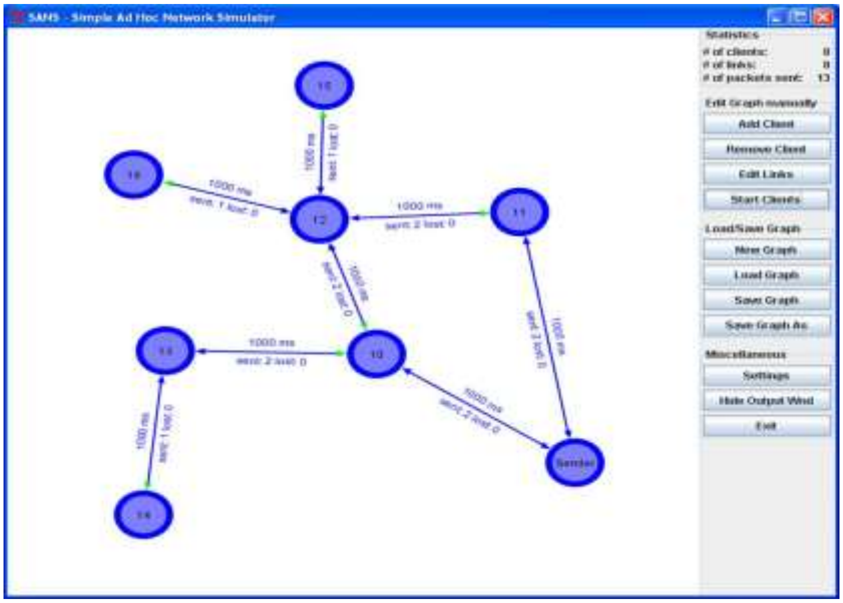


Figure 2: working scenario with OMNET++ [15]

However, the evaluation module continuously collects information about different events during the simulation (e.g., message was sent or received, connection was established or released, etc.) in a log file. Using the data stored in the log file and the filters working on them appropriate graphs can be generated or the whole simulation can be played back step by step or faster than the simulation speed. The simulation environment supports statistic data collecting. It provides some statistical calculations on the collected data for example: minimum value, maximum value, mean, deviation, average and also histograms can be displayed [16].

4.2 SANS: SANS run the simulation framework and all simulated client programs within one common Java Virtual Machine. As a consequence name collisions between the active clients need to be prevented to guarantee the absence of hidden communication channels (for example through static variables). The only secure way to assure such separation is to grant each node an individual namespace. SANS loads each client in a new custom class loader which automatically generates a new namespace for the client. As a result the system has a slightly higher memory usage, since some classes are loaded multiple times but it allows the usage of static methods and fields in the client code without any interference between the different simulated applications [13] which is one of key points on using SANS. Following figure shows the flooding example of SANS.



SANS - Simple Ad Hoc Network Simulator

Statistics
# of clients: 8
# of links: 8
# of packets sent: 13

Figure 1: SANS: Flooding Example [13].

5. CONCLUSION

Mobile ad hoc networks typically used in military and disaster relief purposes for its flexibility and fast system deployment. Nowadays, it is becoming more popular for its unique properties. Those properties are: no fixed infrastructure, dynamic change in topology, limited bandwidth, faster deployment and low setup cost. In this research, we have provided a detail literature of a framework for better security in dealing with threats like hacking, threat in money transfer issues, leakage of confidential information. We are very much confident on sustainability of our proposed model among mobile network community.

REFERENCES

[1] "Mobile Ad Hoc Networking," *Cisco*. [Online]. Available: https://www.cisco.com/c/en/us/products/ios-nx-os-software/mobile-ad-hoc-networking/index.html. [Accessed: 04-Sep-2018].

[2] A. Dorri, S. R. Kamel, and E. Kheyrkhah, "SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY," *Int. J. Comput. Sci. Eng. Surv.*, vol. 6, no. 1, Feb. 2015.

[3] L. Scialabba, "SECURING THE MOBILE NETWORK," *AVIAT Netw. Solut. Mark.*, p. 10, Sep. 2013.

[4] R. Kumar, Geethanjali, and R. Babu, "Security issues in Mobile Ad-Hoc Networks," *Int. J. Eng. Invent.*, vol. 2, no. 11, pp. 48–53, Jul. 2013.

[5] S. Sen, J. Clark, and J. Tapiador, "Security Threats in Mobile Ad Hoc Networks." Department of Computer Science, University of York, YO10 5DD, UK.

[6] Priti and P. Sharma, "A Review: Security Issues in Mobile Ad Hoc Network," *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 5, pp. 365–370, May 2014.

[7] "Integrated Mobile Secure (IMS)," *Infinitium*. [Online]. Available: http://www.infinitium.com/page/171/Integrated-Mobile-Secure-(IMS)/. [Accessed: 06-Sep-2018].

[8] Malgo, "3-D Secure – Advantages and Disadvantages for Merchants." Across the Board, Blog on e-business and online payments.

[9] "The Network Simulator - ns-2." [Online]. Available: https://www.isi.edu/nsnam/ns/. [Accessed: 11-Sep-2018].

[10] "Ns2 Code for Mobile Ad Hoc Network using NS2 Simulator," *NS2 Simulator Projects*. .

[11] "OMNeT++ - Simulation Manual." [Online]. Available: https://omnetpp.org/doc/omnetpp/manual/. [Accessed: 11-Sep-2018].

[12] V. Manchikalapudi and K. Babu, "Simulation of Efficiency in Mobile Ad Hoc Networks using OMNeT++," *Res. J. Appl. Sci. Eng. Technol.*, vol. 10, no. 10, pp. 1192–1196, Aug. 2015.

[13] N. Burri, R. Wattenhofer, Y. Weber, and A. Zollinger, "SANS: A Simple Ad Hoc Network Simulator," *Comput. Eng. Netw. Lab. ETH Zurich Switz.*

[14] "16.1.1 Mobilenode: creating wireless topology." [Online]. Available: https://www.isi.edu/nsnam/ns/doc/node171.html#fig:mobilenode-dsdv. [Accessed: 11-Sep-2018].

[15] Omnet Manual, "OMNeT++ Ad Hoc Simulation Projects." Ad Hoc Network simulation Projects Using OMNeT++ simulator.

[16] S. Imre, C. Keszei, D. Hollós, P. Barta, and C. Kujbus, "Simulation Environment for Ad-Hoc Networks in OMNeT++." Department of Telecommunications Budapest University of Technology and Economics, Pazmany P. 1/D, Budapest, H-1117.