ISSN : 0976-8491(Online) | ISSN : 2229-4333(Print)

Analysis of Different Propagation Model for IPSec-LANMAR Routing Protocol to Secure Network Layer for MANET in Emergency Area Environment

[1]D.Devi Aruna, [2]Dr.P.Subashini

[1,2]Dept. of Computer Science, Avinashilingam Deemed University for Women, Coimbatore, India

Abstract

Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes, which dynamically exchange data among themselves without the reliance of a fixed base station. It have potential use in a wide variety of disparate situations such as responses to hurricane, tsunami, earthquake, emergency relief, terrorism and military operations. In this work, investigations on the behavior of IPSec-LANMAR routing protocol with propagation models that take into account two main characteristics of the wireless channel – path loss and shadowing is presented. The choice of radio propagation models with IPSec-LANMAR also has a strong impact on the performance of a protocol because the propagation model determines the number of nodes within one collision domain, an important input for contention and interference. This, in turn, has a direct effect on a node's ability to transmit a packet to another node and it provide security services for both routing information and data message at network layer. The simulation result shows that Free space propagation model with IPSec-LANMAR routing protocol outperforms compared to Two ray propagation model and Shadowing model in emergency area environment and the experiments are carried out using the simulator Qualnet version 5 also the performance of propagation models with IPSec-LANMAR for MANETs is compared based on different parameter metrics.

Key Words

MANET, IPSec, LANMAR, Propagation model, Network layer security

I. Introduction

Mobile Ad-hoc Network (MANET) holds the promise of an anytime, anywhere connection to information in areas that have little or no infrastructure. Rescuers, soldiers in the battlefield, or even ordinary folk on a fishing trip could access the information they need by connecting to other wireless units forming a network. Networks could be set up quickly in industrial areas or historical buildings where it would be very difficult or impossible to put together a wired infrastructure.MANETs are extremely vulnerable to various attacks. It is observed that MANETs show vulnerabilities across all network protocol layers, especially the routing protocol at network layer. The proposed method has a strong impact on the performance of a protocol and it provide security services for both routing information and data message at network layer emergency area environment [1, 2].

The paper is organized in such a way that Section 2 discusses overview of routing protocol and IPSec in MANETs for network layer security, SectionIII explains overview of Propagation Model, Section4 contains description of Emergency Area Scenarios and the Simulation model, Section6 contains the conclusion of the paper.

II. Overview of Routing Protocol and IPSec in MANETs for Network Layer Security

This section briefly describes different types of routing protocols and IPSec in MANETs for network layer security.

A. Routing Protocols

The fundamental idea of a routing protocol is to deliver the messages from source to destination with enhanced performance in terms of delay and security. Routing protocols may be generally categorized as,

(I) Table driven Protocol and

(II) Source initiated demand driven Protocol

1. Table Driven Protocols

Table driven protocols maintain consistent and up to date routing information about each node in the network. These protocols require each node to store their routing information and when there is a change in network topology updating has to be made throughout the network. Some of the existing table driven protocols are,

- Landmark Ad-Hoc Routing(LANMAR)
- Fisheye State Routing protocol (FSR)
- Optimized Link State Routing protocol (OLSR)
- Destination sequenced Distance vector routing (DSDV)

2. Source Initiated Demand Driven Protocols

In demand driven routing protocols, routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destinations. The route remains valid till the destination is reachable or until the route is no longer needed [3, 6].

The different types of On Demand driven protocols are:

- Ad hoc On Demand Distance Vector (AODV)
- Dynamic Source routing protocol (DSR) and
- Temporally ordered routing algorithm (TORA)

Landmark Adhoc Routing (LANMAR) is mostly used in MANET and the same is taken for study in proposed work. A brief description of the LANMAR routing protocol is given below.

3. Landmark ad-hoc routing (LANMAR)

LANMAR is an efficient routing protocol in a "flat" ad hoc wireless network. LANMAR assumes that the large scale ad hoc network is grouped into logical subnets in which the members have a commonality of interests and are likely to move as a "group". LANMAR uses the notion of landmarks to keep track of such logical subnets. Each logical group has one node serving as landmark. The route to a landmark is propagated throughout the network using a Distance Vector mechanism. The routing update of LANMAR can be explained as follows: Each node periodically exchanges topology information with its immediate neighbors. In each update, the node sends entries within its fisheye scope. Updates from each source are sequentially numbered. To the update, the source also piggybacks a distance vector of all landmarks. Through this exchange process, the

table entries with larger sequence numbers replace the ones with smaller sequence numbers. As a result, each node has detailed topology information about nodes within its fisheye scope and has a distance and routing vector to all landmarks [3, 6].

4. IPSec in MANETS for network layer security

IP security (IPSec) developed by Internet Engineering Task Force (IETF) is a suite of protocols used to secure traffic at the IP layer. The main protocol components of IPSec are Authentication Header (AH) and Encapsulating Security Payload (ESP), which describe the IP header extensions for carrying cryptographically protected data, and Internet Key Exchange (IKE). IPSec is based on Security Associations (SAs). A security association is a simplex connection whose traffic is protected by security service designated by parameters such as the encryption algorithm, keys, and lifetime. SA is uniquely identified by a tuple of Security Parameter Index (SPI), destination IP address, and IPSec protocol (AH or ESP). IPSec protocol is based on the establishment of Security Association between packet sender and receiver. SA is set up in the IKE phase by Diffie- Hellman (DH) algorithm. Although DH algorithm is subject to man-in-the-middle attack, this problem could be alleviated in most of the Ad Hoc network application scenarios due to the following reasons: The nodes can always be pre-assigned with certain initial shared secret by their manufacturer; these secrets can be used at the initial IKE phase to authenticate the validity of the DH connections. This pre-configured shared secret can then be available in most MANET systems, and is essential for adopting IPSec secure communications and membership verification. Upon the establishment of membership management mechanism and the corresponding trust model in MANET, IPSec can be an appropriate choice for MANET network layer to protect both routing information and data message. For IPsec to work, communication entities must share a public key. This key exchange process is accomplished through key management mechanisms that refer to the creation, distribution, installation, authentication, and access control of the keying material. A number of cryptographic algorithms are also specified in IPsec for authentication and encryption.

III. Overview of Propagation models

This chapter briefly describes different types of propagation models.

A. Free Space Propagation Model

The free space propagation model is the simplest path loss model in which there is a direct path signal between the transmitter and the receiver, with no atmospheric attenuation or multipath components. In this model the relationship between the transmitted power Pt and the received power Pr is given by

$$P_r = P_t G_t G_r (\lambda/4\Pi d)^2 \quad (1)$$

where Gt and Gr are the transmitter and receiver antenna gains, respectively, in the direction from the transmitter and receiver, d is the distance between the transmitter and receiver, and λ=c/f is the wavelength of the signal. Realistic path loss models that take into account the propagation effects in specific environments can be obtained by solving Maxwell's equations. Since obtaining solutions for such models involves complex algorithms and computation intensive operations, simpler models have been proposed to depict the loss [1, 4].

B. Two Rays Propagation Model

Another popular path loss model is the two-ray model or the two-path model. The free space model described above assumes that there is only one single path from the transmitter to the receiver. But in reality the signal reaches the receiver through multiple paths (because of reflection, refraction and scattering). The two-path model tries to capture this phenomenon. The model assumes that the signal reaches the receiver through two paths, one a line-of-sight path, and the other the path through which the reflected (or refracted, or scattered) wave is received. According to the two-path model, the received power is given by

$$P_r = P_t G_t G_r (h_t h_r / d^2)^2 \quad (2)$$

Where Pr is the transmitted power, Gt and Gr are the transmitter and receiver antenna gains, respectively, in the direction from the transmitter and receiver, d is the distance between the transmitter and receiver, and ht and hr are the heights of the transmitter and receiver, respectively [1, 5].

C. Shadowing Model

Fading refers to the fluctuations in signal strength when received at the receiver. Fading can be classified into two types: fast fading and slow fading. Fast fading refers to the rapid fluctuations in the amplitude, phase, or multipath delays of the received signal, due to the interference between multiple versions of the same transmitted signal arriving at the receiver in slightly different times. Slow fading occurs when objects transmissions lie partially between the transmitter and receiver. Slow fading may occur when the receiver is inside a building and the radio wave must pass through the walls of a building, or when the receiver is temporarily shielded from the transmitter by a building. Slow fading is also referred to as shadow fading (shadowing) since the objects that cause the fade, which may be large buildings or other structures, block the direct transmission path from the transmitter to the receiver [7, 8, 10].

IV. Simulation Model

MANETs have found practical applications in emergencies that need a quick network to be established between members of emergency services. This type of MANET makes use of the cars, laptops, PDAs and high-tech cellular phones (HTC) as routers to direct information to the desired destination.

To evaluate the impact of the radio wave propagation model on the performance of a Mobile Ad Hoc Network. In this work, emergency area scenarios consists of 100 wireless nodes forming an ad hoc network, moving over a 1500 X 1500 flat space, Network traffic is created by starting CBR connections between randomly selected nodes. The simulation duration is 1000 sec. simulations ran with movement patterns generated for 4 different maximum speeds, 20, 40, 60, 80 m/sec. fig. 1, shows emergency area scenario.

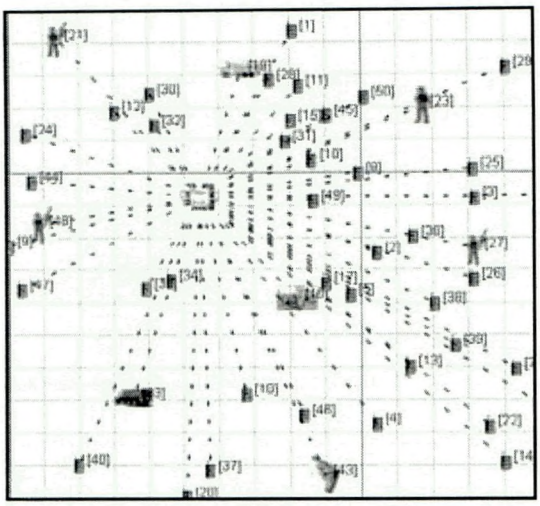

Fig. 1: Emergency Area Scenario

The above simulation model based on QualNet 5 [9] has been created for the evaluation. Performance evaluations are based on the simulations of 100 wireless mobile nodes that form a vireless ad hoc network over a rectangular (1500 X 1500 m) lat space. The MAC layer protocol used in the simulations was the Distributed Coordination Function (DCF) of IEEE 802.11. In these simulations, results corresponding to four metrics namely, packet delivery ratio, throughput, end-to-end delay, and jitter has been evaluated.

A. Packet Delivery ratio

The packet delivery ratio (PDR) of a receiver is defined as the ratio of the number of data packets actually received over the number of data packets transmitted by the senders. The average packet delivery ratio is the average of the packet delivery ratios taken over all the receivers.

B. End-to-End delay

The end-to-end delay of a packet is defined as the time a packet takes to travel from the source to the destination. The average end-to-end delay is the average of the end-to-end delays taken over all the received packets Eqn (3) is used to find the end to ıd delay of the packet.

$$delay = \frac{1}{nbx} \sum_{i \in x} \sum_{iey} \frac{delay_j}{nby} \quad (3)$$

where x is the set of destination nodes that received data packets, nbx is the number of receiver nodes and y is the set of packets received by node i as the final destination.

C. Throughput

The throughput of a receiver (per-receiver throughput) is defined as the ratio of the number of bits received over the time difference between the first and the last received packets. The average throughput is the average of the per-receiver throughputs taken over all the receivers. Eqn (4) is used to find the throughput of the packet.

$$Throuhput(\%) = \frac{\text{Re}ceivedpackets}{Sentpackets} * 100 \quad (4)$$

Delay jitter: Delay jitter is the variation (difference) of the inter-arrival times between the two successive packets received. Each receiver calculates the average per-source delay jitter from the received packets originated from the same source. The receiver then takes the average over all the sources to obtain the average per-receiver delay jitter. The average delay jitter is the average of the per-receiver delay jitters taken over all the receivers

V. Analysis of results

The analysis of simulation results is performed based on the standard metrics with varying speed between different radio propagation models.

Fig. 2, indicates that Free space and Two ray ground models are performing better than Shadowing model when packet delivery ratio is considered as metric.

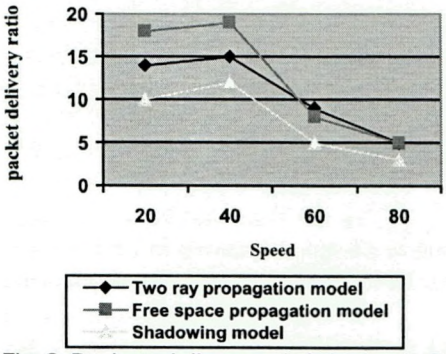

Fig. 2: Packets delivery ratio is higher in Free space propagation IPSec-LANMAR when compared to Two ray ground model and Shadowing model.

Fig. 3: indicates Two ray ground models and Free space model are performing better than Shadowing model when jitter is considered as metric.

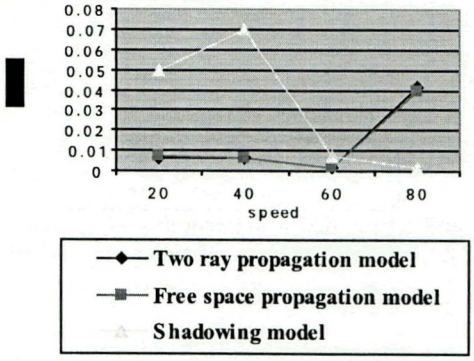

Fig. 3: Jitter is lower in Free space propagation model with IPSec-LANMAR when compared to Two ray ground model and Shadowing model.

Fig. 4: indicates Two ray ground models and Free space model are performing better than Shadowing model when End to End delay is considered as metric.

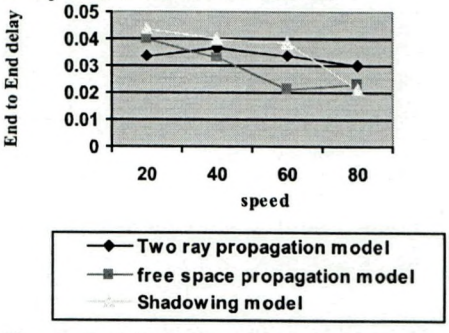

Fig. 4: End to End delay is lower in Free space propagation model with IPSec-LANMAR when compared to Two ray ground model and Shadowing model.

Fig. 5: indicates Two ray ground models and Free space model are performing better than Shadowing model when throughput is considered as metric.

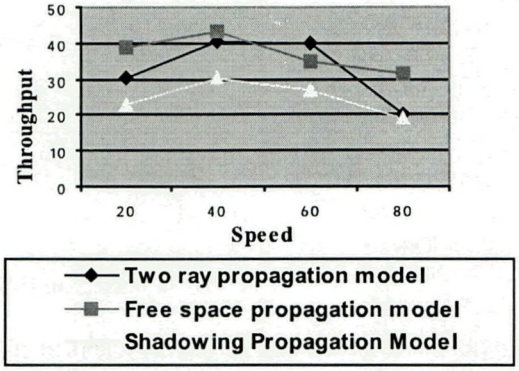

Fig. 5: Throughput is higher in Free space propagation model with IPSec-LANMAR when compared to Two ray ground model and Shadowing model.

VI. Conclusion

Mobile ad hoc networks (MANETs) consist of a collection of vireless mobile nodes, which dynamically exchange data among .hemselves without the reliance on a fixed base station. In this work, investigations is done on the behavior of IPSec- LANMAR routing protocol with propagation models that take into account two main characteristics of the wireless channel – path loss and shadowing. The choice of radio propagation models with IPSec-LANMAR also has a strong impact on the performance of a protocol because the propagation model determines the number of nodes within one collision domain, an important input for contention and interference. This, in turn, has a direct effect on a node's ability to transmit a packet to another node and it provide security services for both routing information and data message at network layer. The simulation result shows that free space propagation model with IPSec-LANMAR routing protocol outperforms compared to two ray propagation model and shadowing model in emergency area scenarios.

eferences

[1] Ayyaswamy Kathirvel, Rengaramanujam Srinivasan ,"Analysis of Propagation Model using Mobile Ad Hoc Network Routing Protocols," International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 1, No. 1, 2010.

[2] Tapan K. Sarkar, Zhong Ji, Kyungjung Kim, Abdellatif Medour, "A Survey of Various Propagation Models for Mobile Communication," IEEE Antennas and Propagation Magazine, Vol.45, No. 3, June 2003.

[3] Ashwini K. Pandey, Hiroshi Fujinoki, "Study of MANET routing protocols by Glomosim simulator", International Journal of Network Management, pp. 393–410.

[4] Martinez, F.J., Chai-Keong Toh, Cano, J.C., Calafate, C.T., Manzoni, P., Univ. of Zaragoza, "Realistic Radio Propagation Models (RPMs) for VANET Simulations", appears in: Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE Issue 2009 On pp. (s): 1 – 6

[5] Mineo Takai, Jay Martin, Rajive Bagrodia, "Effects of wireless physical layer modeling in mobile ad hoc networks", In Proceedings of MobiHoc 2001, pp. 87–94. ACM Press, 2001.

[6] Ingo Gruber, Oliver Knauf, Hui Li, "Performance of Ad Hoc Routing Protocols in Urban Environments", In Proceedings of European Wireless 2004 (EW'2004, Barcelona, Spain,February 24 - 27, 2004, Barcelona, Spain

[7] Nagendra sah, Amit Kumar, "CSP Algorithm in Predicting and Optimizing the Path Loss of Wireless Empirical Propagation Models", International Journal of Computer and Electrical Engineering, Vol. 1, No. 4, October, 2009.

[8] K. Rizk, "Propagation in Microcellular and Small Cell Urban Environment", PhD thesis, Swiss Federal Institute of Technology of Lausanne, 1997.

[9] Scalable Network Technologies. The QualNet simulator [Online] Available: http://www.qualnet.com/.

[10] Arne Schmitz, Martin Wenig,"The Effect of the Radio Wave Propagation Model in Mobile AdHocNetworks",Torremoli nos,Malga,Spain,MSWiM'06,October 2-6,2006

Ms.D.Devi Aruna. received MCA Degree from Avinashilingam Deemed University for Women, Coimbatore in 2008 respectively and pursuing her Ph.D in same University. She has three years of research experience in UGC project. Her research interests are cryptography and Network Security. She has 9 publications at national and international level.

Dr. P. Subashini, Associate Professor, Dept. of Computer Science, Avinashilingam Deemed University has 18 years of teaching and research experience. Her research has spanned a large number of disciplines like Image analysis, Pattern recognition, neural networks, and applications to Digital Image processing. Under her supervision she has seven research project of worth one crore from various funding agencies like DRDO, DST and UGC.