DSSS with ISAKMP Key Management Protocol to Secure Physical Layer for Mobile Adhoc Network

Dr.G.Padmavathi[1], Dr.P.Subashini[2], and Ms.D.Devi Aruna[3]
[1]Professor and Head, Department of Computer Science,
Avinashiligam University for Women, Coimbatore – 641 043
ganapathi.padmavathi@gmail.com
[2]Associate Professor, Department of Computer Science,
Avinashilingam University for Women, Coimbatore – 641 043
mail.p.subashini@gmail.com
[3]Project fellow, Department of Computer Science,
Avinashiligam University for Women, Coimbatore – 641 043
deviaruna2007@gmail.com

ABSTRACT

The wireless and dynamic nature of mobile ad hoc networks (MANETs) leaves them more vulnerable to security attacks than their wired counterparts. The nodes act both as routers and as communication end points. This makes the physical layer more prone to security attacks. The MANET physical layer is challenging to DoS attack and also some passive attacks. The physical layer protocol in MANETs is responsible for bit-level transmission between network nodes. The proposed model combines spread spectrum technology Direct Sequence Spread Spectrum (DSSS) with key management technique ISAKMP to defend against signal jamming denial-of-service attacks in physical layer of MANET.DSSS with ISAKMP is found to be a good security solution even with its known security problems. The simulation is done using network simulator qualnet 5.0 for different number of mobile nodes. The proposed model has shown improved results in terms of Average throughput, Average end to end delay, Average packet delivery ratio, and Average jitter.

KEYWORDS

MANET, DSSS, ISAKMP, Denial of Service attack

1. Introduction

Mobile Ad hoc Networks (MANETs) present communication over a shared wireless channel without any pre-existing infrastructure. Communications must be set up and maintained on the fly over mostly by wireless links. In ad hoc network each node can both route and forward data. Security has become a main concern to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wireline networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. It includes shared wireless medium, stringent resource constraints, open network architecture and highly dynamic network topology. So, the existing security solutions for wired networks do not openly apply to the MANET domain. The vital goal of the security solutions for MANETs is to provide security services, such as

confidentiality, integrity, anonymity, authentication and availability, to mobile users. To achieve the goals, the security solution spanning the entire protocol stack. DoS attacks can be launched against any layer in the network protocol stack [8][9]. The physical layer must get used to rapid changes in link characteristics. Physical layer security is important for securing *MANET* as many attacks can take place in this layer. Moreover an attacker can overhear or disrupt the service of wireless network physically.The proposed model combines spread spectrum technology Direct Sequence Spread Spectrum (DSSS) with key management technique ISAKMP to defend against signal jamming denial-of-service attacks in physical layers of MANET. Table 1 describes the security issues in each layer.

TABLE 1: LAYERWISE SECURITY CHALLENGES

Layer	**Security issues**
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

The paper is organized in such a way that Chapter 2 discusses Review of Literature, Chapter 3 discusses proposed method, Chapter 4 discusses Experimental evaluation and Chapter 5 gives the conclusion

2. REVIEW OF LITERATURE

This chapter briefly describes Denial of Service attacks for MANET and related work.

2.1. Denial of Service attack

An attacker attempts to avoid authorized and legitimate users from the services offered by the network. The typical way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operate in the manner in which it is designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. DoS attacks can be launched against any layer in the network protocol stack. On the physical and MAC layers, an adversary

could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bring down critical services such as the key management service. For example, consider the following: In figure1 assume a shortest path that exists from **S** to **X** and **C** and **X** cannot hear each other, that nodes **B** and **C** cannot hear each other, and that **M** is a malicious node attempting a denial of service attack. Suppose **S** wishes to communicate with **X** and that **S** has an unexpired route to **X** in its route cache. **S** transmits a data packet towards **X** with the source route **S --> A --> B --> M --> C --> D --> X** contained in the packet's header. When **M** receives the packet, it can alter the source route in the packet's header, such as deleting **D** from the source route. Consequently, when **C** receives the altered packet, it attempts to forward the packet to **X**. Since **X** cannot hear **C**, the transmission is unsuccessful [6][7][9][10].

S ↔A↔ B↔ M ↔C↔ D↔ X

Figure 1: Denial of Service attack

3. PROPOSED METHOD

This chapter describes proposed method combines Direct Sequence Spread Spectrum (DSSS) with key management technique ISAKMP in Mobile Adhoc Networks.

3.1. Direct Sequence Spread Spectrum (**DSSS**) is a modulation technique. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated.

Features

DSSS phase-modulates a sine wave pseudo randomly with a continuous string of pseudo noise (PN) code symbols called "chips", each of which has a much shorter duration than an information bit. That is, each information bit is modulated by a sequence of much faster chips. Therefore, the chip rate is much higher than the information signal bit rate.

DSSS uses a signal structure in which the sequence of chips produced by the transmitter is known *a priori* by the receiver. The receiver can then use the same PN sequence to counteract the effect of the PN sequence on the received signal in order to reconstruct the information signal.

3.2. Internet Security Association and Key Management Protocol (ISAKMP)

Internet Security Association and Key Management Protocol (ISAKMP) combine the security concepts of key management, authentication, and security associations to establish the required security for private communications on the Internet. The Internet Security Association and Key

Management Protocol (ISAKMP) defines packet format and procedures to negotiate, modify, establish and delete Security Associations (SAs). ISAKMP defines payloads for exchanging key generation and authentication data. ISAKMP is separate from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. Separating the functionality into three parts adds difficulty to the security analysis of a complete ISAKMP implementation. However, the separation is vital for interoperability between systems with differing security requirements and should also simplify the analysis of further evolution of an ISAKMP server. ISAKMP is intended to support the negotiation of SAs for security protocols at all layers of the network stack Within ISAKMP, a Domain of Interpretation (DOI) is used to group related protocols, using ISAKMP to negotiate security associations. Security protocols sharing a DOI choose security protocol and cryptographic transforms from a common namespace and share key exchange protocol identifiers. They also share a common interpretation of DOI-specific payload data content, including the Security Association and Identification payloads [3][4][5].

4. Experimentation and Evaluation

Qualnet5.0 network simulator is used for experimentation. Mobility scenarios are generated using a Random waypoint model by varying 10 to 50 nodes moving in a terrain area of 1500m x 1500m.The simulation is made to analyze the performance of the network's various parameters. The metrics used to evaluate the performance are:

1) Average packet delivery ratio

2) Average end-to-end delay

3) Average delay jitter

4) Average throughput

Average 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.

Average end-to-end delay: The end-to-end delay of a packet is defined as a packet takes a time 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 (1) is used to find the end to end delay of the packet.

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

x: is the set of destination nodes that received data packets.

nbx: is the number of receiver nodes

y: is the set of packets received by node i as the final destination.

Average 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.

Average throughput: The throughput of a receiver (per-receiver throughput) is defined as the ratio 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 (2) is used to find the throughput of the packet.

$$Throuhput(\%) = \frac{\text{Re}\,ceivedpackets}{Sentpackets} * 100 \text{ ---(2)}$$

Performance comparison of routing protocol DSSS with ISAKMP routing protocol with denial of service attack.

The different parameters are considered for evaluation. Average packet delivery ratio, Average throughput, should be higher and Average end-to-end delay, Average delay jitter must be lower.

Figure2 shows that Average packet delivery ratio is higher in ISAKMP with DSSS for denial of service attack compared to DSSS.

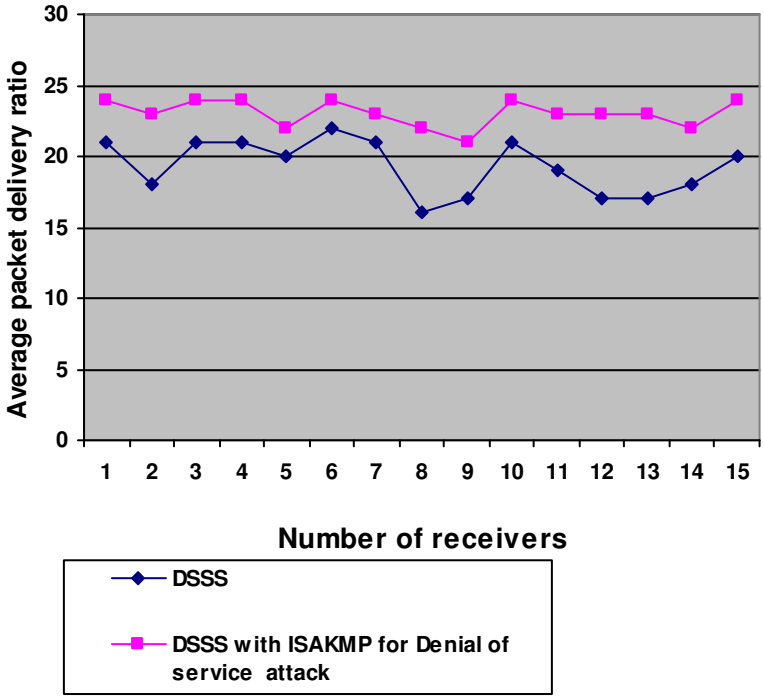

Figure2: Comparison of Average packet delivery ratio of ISAKMP with DSSS FOR denial of service attack compared to DSSS.

Figure 3 shows that End to End Delay is lower in ISAKMP with DSSS FOR denial of service attack compared to DSSS.

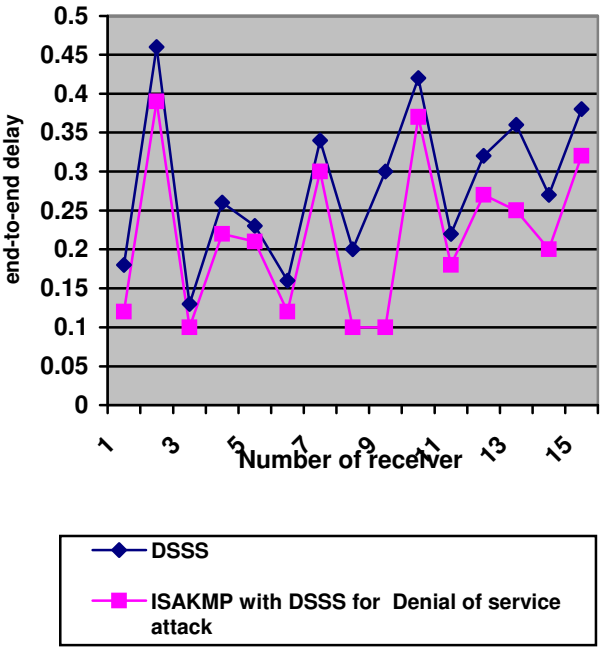

Figure 3: Comparison of End to End delay of ISAKMP with DSSS FOR denial of service attack compared to DSSS.

Figure4 shows that Throughput is higher in ISAKMP with DSSS FOR denial of service attack compared to DSSS.

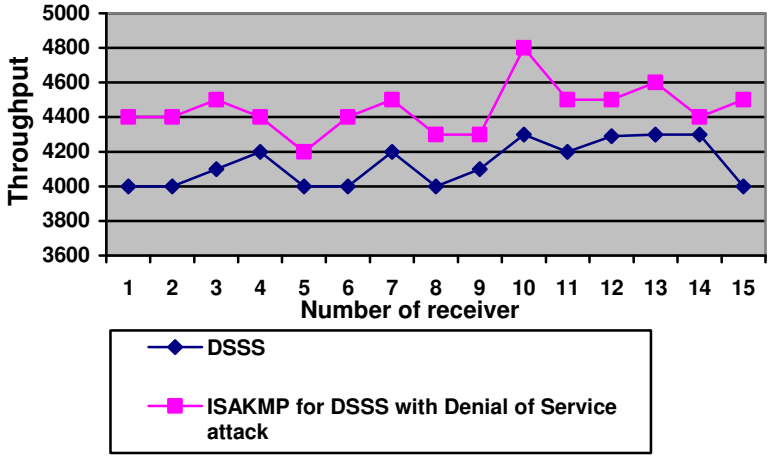

Figure4: Comparison of Throughput ISAKMP with DSSS FOR denial of service attack compared to DSSS.

Figure5 shows that Average Jitter is lower in ISAKMP with DSSS FOR denial of service attack compared to DSSS.

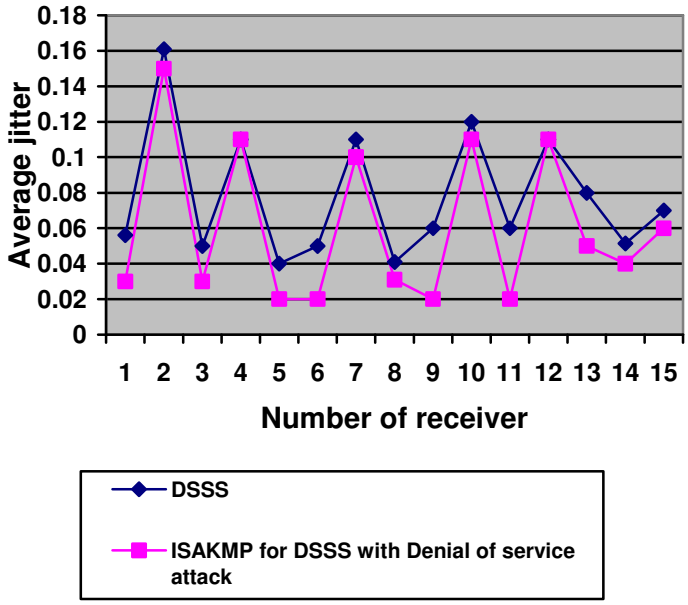

Figure5: Comparison of a Average Jitter ISAKMP with DSSS FOR denial of service attack compared to DSSS.

It is observed that proposed model is strong against denial of service attack in physical layer of MANET.

5. CONCLUSION

Mobile Adhoc network is a collection of mobile nodes without infrastructure. During deployment, security emerges as a central requirement due to many attacks that affects the performance of the ad hoc networks. The MANET physical layer is resistant to DoS attack and also some passive attacks. The physical layer protocol in MANETs is responsible for bit-level transmission between network nodes. The proposed model combines spread spectrum technology Direct Sequence Spread Spectrum (DSSS)with key management technique ISAKMP to defend against denial of service attacks in physical layers of MANET. *DSSS* with ISAKMP is found to be a good security solution even with its known security problems. The proposed model has shown better results in terms of Average packet delivery ratio, Average throughput, Average end to end delay and Average jitter.

References

1. IEEE Standard 802.3, “Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD), Access Method and Physical Layer Specifications,” 2000 Edition.

2.IEEE Standard 802.11b-1999 (Supplement to ANSI/IEEE Standard 802.11, 1999 Edition).

3. Maughan, M. Schertler, M. Schneider, and J. Turner. Internet security association and key management protocol (ISAKMP). RFC 2408, Internet Engineering Task Force, November 1998.

4. Joshua D. Guttmann, Amy L. Herzog, and F. Javier Thayer**,"** *Authentication and Confidentiality via IPsec*" Springer LNCS, 30 June 2000.

5. Matt Blaze, John Ioannidis, Angelos D. Keromytis*,"Trust Management for IPsec"* Dept. of Electrical & Computer Engineering, Michigan Tech, Houghton, 103 – 118, 1999

6.Manel Guerrero Zapata, N. Asokan *"Securing ad hoc routing protocols",* Proceedings of the ACM workshop on Wireless security.,2002

7. 1.Hoang Lan Nguyen, Uyen Trang Ngu," A study of different types of attacks on multicast in mobile ad hoc networks" ,Elsevier journal –No. 6 (2008) pg 32–46.

8. A.D. wood and J.A. Stankovic, "Denial of Service in Sensor Networks," IEEE October 2002.

9.M.K. Denko, "A Localized Architecture for Detecting Denial of Service (DoS) Attacks in Wireless Ad Hoc Networks", In Proc. IFIP INTELLCOMM'05, Montreal, Canada

10. I. Aad, J.P, Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks", ACM MOBICOM 2004, Philadelphia, PA, USA.

Dr. Padmavathi Ganapathi is the Professor and Head of Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 23 years of teaching experience and one year Industrial experience. Her areas of interest include Network security and Cryptography and real time communication. She has more than 110 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA.

Dr. Subashini is the Associate professor in Department of Computer Science, Avinashilingam Deemed University for Women, Coimbatore. She has 18 years of teaching experience. Her areas of interest include Object oriented technology, Data mining, Image processing, Pattern recognition. She has 95 publications at national and International level**.**

Ms.D.Devi Aruna. received MCA Degree from Avinashilingam University for Women, Coimbatore in 2008 respectively and pursuing her Ph.D in same University. She is currently working as a Project Fellow in UGC project in Department of Computer Science in the same University and has three year of research experience. Her research interests are cryptography and Network Security. She has 12 publications at national and international level.