Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol 2, No.2, 2012

Intrusion Detection Protocol for Adhoc Networks

Sunil Taneja[1*] Ashwani Kush[2]

1. Department of Computer Science, Smt. Aruna Asaf Ali Government Post Graduate College, Kalka, India
2. Department of Computer Science, University College, Kurukshetra University, Kurukshetra, India

* E-mail of the corresponding author: suniltaneja.iitd@gmail.com

Abstract

MANET is accessible to legitimate as well as non- legitimate network users. Secured routing over such kind of network is a very critical task due to highly dynamic environment. In this research paper, a new intrusion detection protocol has been proposed for secured routing over MANET. An experimental analysis of proposed protocol has been carried using network simulator. Based on the experimental analysis, recommendations have been made about the significance of protocol under various situations.

Keywords: Adhoc, Intrusion, MANET, Network, Routing, Secured

1. Introduction

MANET can be viewed as collection of wireless mobile nodes that forms a short-lived network without any fixed infrastructure. In this network, all the nodes configure themselves and are free to move about arbitrarily. The dilemma is that how should it be judged whether the MANET is secure or not. Some of the security attributes (Stallings 2011) that are used to inspect the security state of MANET are availability, integrity, authenticity, confidentiality, authorization and non-repudiation etc. The main threats that violate these security criteria's are generally called as attacks (Stallings 2011) which are divided into two categories: passive vs. active attacks. These attacks are labeled as traffic analysis, eavesdropping, masquerading, message modification, replay and denial-of-service. The prominent characteristics of adhoc networks create challenges in developing complete security solutions. In this paper, efforts are to develop a complete security solution for MANET that has mechanisms for prevention, detection and healing of attacks.

2. Related Work

B. Dahill et al. proposed an on-demand routing protocol ARAN (Dahill et al. 2001) for adhoc networking environment that uses certificates to ensure authentication, integrity and non-repudiation of routing messages. This protocol uses public key cryptography to overwhelm the attacks and ensures secured routing for the managed-open and open adhoc networking environments. A secured routing protocol, SRP, was proposed by P. Papadimitratos and Z. J. Haas (Papadimitratos et al. 2002). It ensures secured communication in the open, collaborative and highly dynamic adhoc networking environment. SRP respond to malicious behavior in a timely manner and ensures comprehensive secure communication. ARIADNE (Perrig et al. 2002) prevents a wide range of attacks to ensure secures routing in an adhoc networking environment. This protocol uses highly efficient symmetric cryptography that makes it more proficient, which in turn prohibits attackers from tampering with uncompromised routes. The problem with this protocol is that it does not safeguard against passive attackers. L. Zhou and Z. J. Haas (Zhou et al. 1999) have used effective key management to ensure secured routing over adhoc networking environment.

S. Marti et al. have used misbehavior detection schemes (Marti et al. 2000) to secure adhoc networks. The problem with this scheme is that it does no guarantee to have two main security parameters viz. integrity and authentication of routing messages. D. B. Johnson et al. (Johnson et al. 2002) proposed to use symmetric cryptography for secured routing over adhoc networking environment and it can be implemented using one way hash chains. Manel Guerrero Zapata, N. Asokan (Zapata et al. 2002) proposed

a secured routing protocol that makes use of asymmetric cryptography to authenticate participating nodes and uses one way hash chains to ensure secured routing over adhoc environment.

3. Proposed Secured Routing Protocol

Efforts have been done to propose a new secured routing protocol for adhoc networking environment. The new protocol has been developed by using the mechanism of hash key chains. Cryptographic hashing (Partow 2007) is used for data/user verification and authentication. The popular examples of hashing functions (Arun 2010) are HMAC, SHA-1 and MD5. The proposed solution ensures safe and secured communication over adhoc environment by applying hashing techniques in different stages of routing.

The hash key chain has been implemented by using a recursive chain (Lamport 1981). First, a random key RK_1 is selected and then the subsequent keys (Kush 2009) are calculated by using the technique of one way hashing as under:

$RK_2 = H [RK_1]$

$RK_3 = H [RK_2]$

……..

……..

……..

$RK_N = [RK_{N-1}]$

A node authenticates any received value on the hash key chain using above-mentioned keys. The received key will be authentic if the computed value is same as that of previously identified authentic key value. Each node over adhoc networking environment discloses the keys in a particular order and the disclosure order is exactly opposite of the keys generation order. Efforts have also been carried out to evaluate the performance of proposed protocol by using a number of quantitative performance metrics.

4. Performance Metrics

RFC 2501 illustrate a number of quantitative metrics that can be used to analyze the performance of MANET routing protocols. Metrics that have been used to analyze the performance of proposed on-demand routing protocol are packet delivery fraction, average end to end delay, network throughput and normalized routing load.

4.1 Packet Delivery Fraction

The packet delivery fraction is defined as the ratio of number of data packets received at the destinations over the number of data packets sent by the sources.

$$\text{Packet Delivery Fraction} = \frac{\text{Total Data Packets Received}}{\text{Total Data Packets Sent}} \text{ X } 100$$

4.2 Average End-to-End Delay

This is the average time involved in delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets.

$$\text{Average End to End Delay} = \frac{\sum (\text{TimeReceived} - \text{TimeSent})}{\text{TotalData PacketsReceived}}$$

4.3 Network Throughput

A network throughput is the average rate at which message is successfully delivered between a destination node (receiver) and source node (sender). It is also referred to as the ratio of the amount of data received

from its sender to the time the last packet reaches its destination. Throughput can be measured as bits per second (bps), packets per second or packet per time slot. For a network, it is required that the throughput is at high-level. Some factors that affect MANET's throughput are unreliable communication, changes in topology, limited energy and bandwidth.

4.4 Normalized Routing Load

The normalized routing load is defined as the fraction of all routing control packets sent by all nodes over the number of received data packets at the destination nodes. In other words, it is the ratio between the total numbers of routing packets sent over the network to the total number of data packets received.

$$\text{Normalized Routing Load} = \frac{\text{Total Routing Packets Sent}}{\text{Total Data Packets Received}}$$

5. Analysis using Performance Metrics

The mobility model used is random waypoint model. An extensive simulation model having scenario of 25 and 85 mobile nodes is used to study inter-layer interactions. Same scenario has been used for performance evaluation of both proposed secured routing protocol and AODV protocol. The packet size is 512 bytes. The square area considered for 25 nodes is 750 meter x 750 meter and 1500 meter x 1500 meter for 85 nodes. The simulation run time for 25 nodes is 500 seconds and 900 seconds for 85 nodes.

5.1 Simulation Results for 25 Nodes having 8 UDP Connections

The pause time has been used as a varying parameter from 100 seconds to 500 seconds and the queue length is 150. The speed for node's movement has been fixed at 5 meters/second. Two malicious nodes have been introduced in the network scenarios which are moving at a speed of one meter per second. Figure 1 shows packet delivery fraction with respect to pause time. The observation is that proposed secured routing protocol gives high packet delivery fraction that AODV. In figure 2, the relationship between average end to end delay and pause time has been depicted. The AODV protocol has high average end to end delay than proposed protocol when the pause time is between 100 to 150 seconds but after that AODV and proposed protocol gives almost same results. On an average, proposed protocol outperforms AODV. The network throughput with respect to pause time has been shown in figure 3. In this figure, proposed protocol gives high throughput than AODV. Therefore, we can say that proposed protocol outperforms AODV in terms of throughput. Figure 4 shows normalized routing load by varying pause time. The bigger this fraction is the less efficient the routing protocol. When the pause time is between 100 seconds to 300 seconds, AODV shows bigger normalized routing load than proposed protocol but after that both proposed protocol and AODV gives almost same results. On an average, proposed protocol outperforms AODV in terms of normalized routing load.

5.2 Simulation Results for 85 Nodes having 16 UDP Connections

The pause time is varying from 100 seconds to 900 seconds and the queue length is same as before. The speed for node's movement has been fixed at 10 meters/second. Two malicious nodes have been introduced in the network scenarios which are moving at a speed of 5 meters/second. Figure 5 shows that packet delivery fraction for proposed secured routing protocol is much higher than that of AODV protocol for all pause times and hence proposed secure routing protocol gives better packet delivery than that of AODV protocol. In figure 6, average end to end delay has been presented with respect to pause time. When the pause time is between 100 seconds to 700 seconds, AODV protocol has elevated average end to end delay than that of proposed protocol but when it is between 700 seconds to 900 seconds, proposed secured routing protocol gives high average end to end delay than AODV.

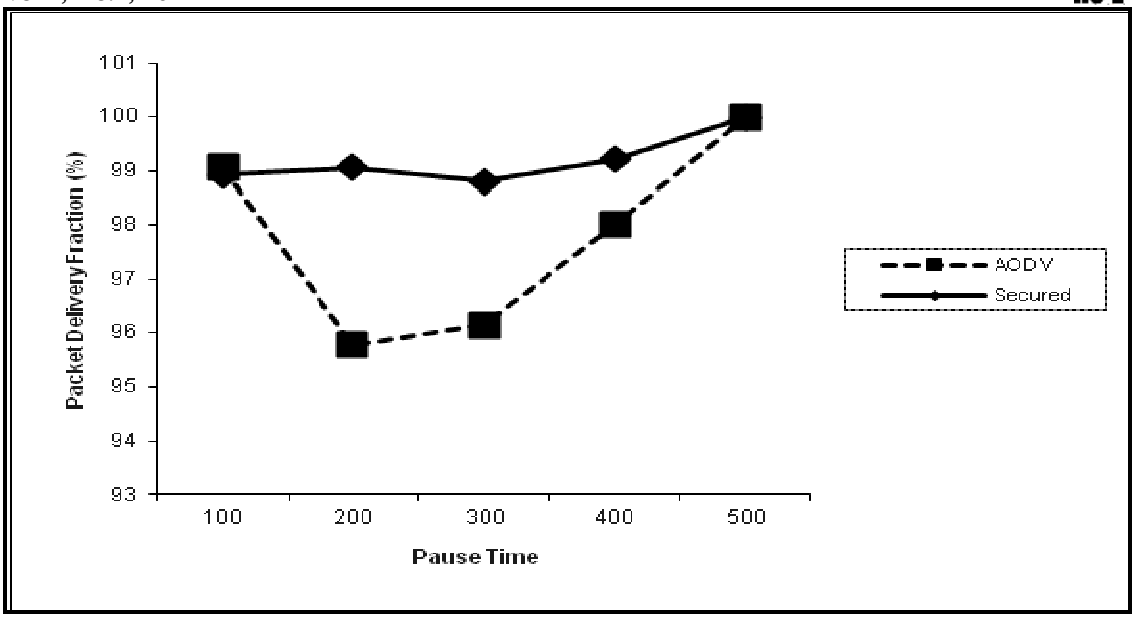

Figure 1. Packet Delivery Fraction

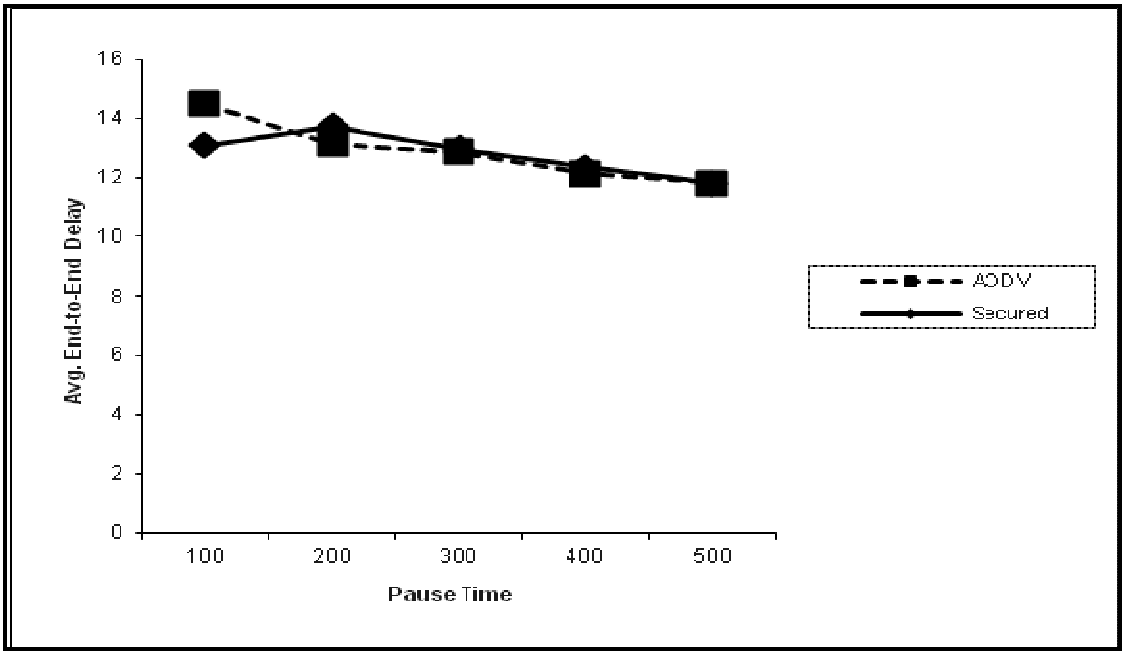

Figure 2. Average End to End Delay

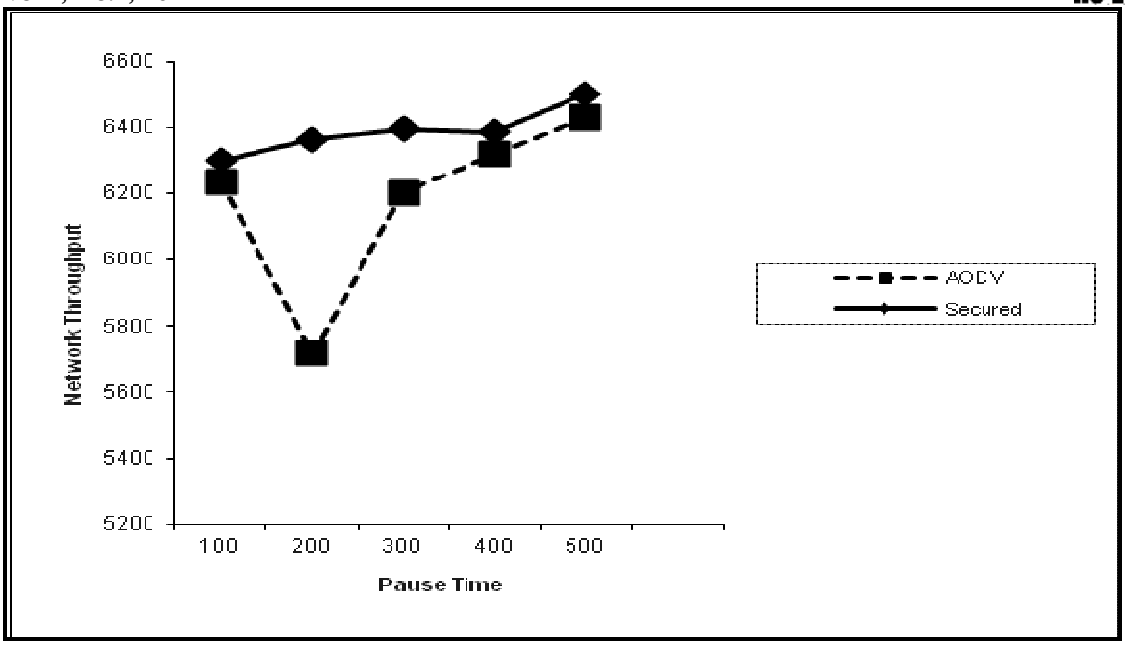

Figure 3. Network Throughput

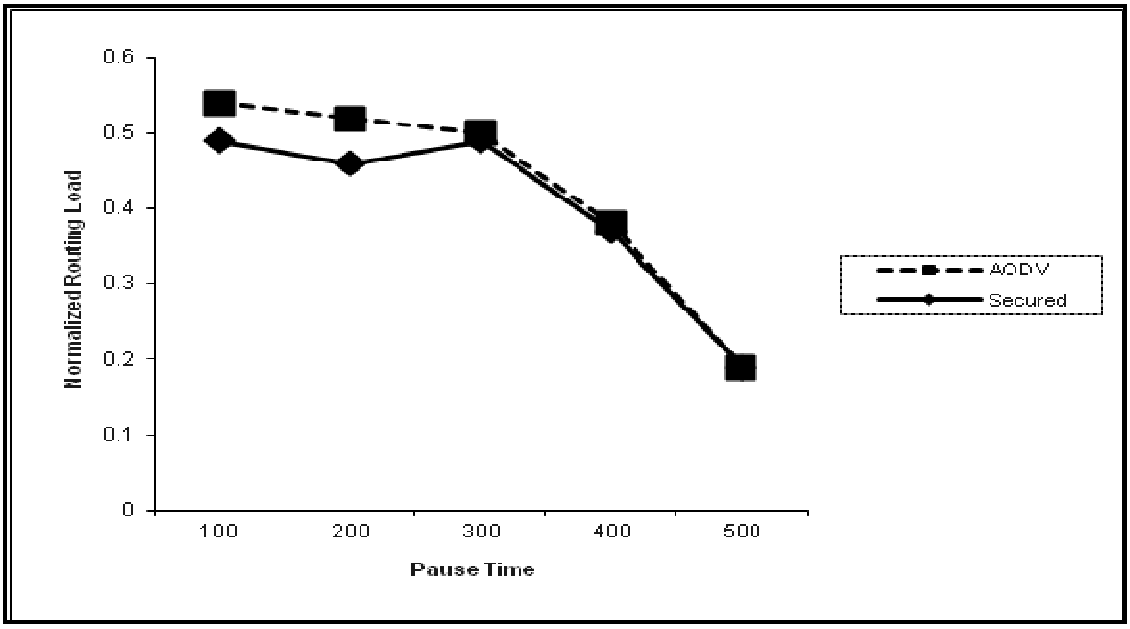

Figure 4. Normalized Routing Load

Concluding, we can say that initially proposed secured routing protocol outperforms AODV but in end AODV starts outperforming proposed secured routing protocol. This issue is still under consideration. Network throughput with respect to pause time has been shown in figure 7. Proposed secured routing protocol gives high throughput than AODV for all pause times and hence proposed secured routing protocol outperforms AODV in terms of better throughput. Figure 8 shows normalized routing load by varying pause time. The bigger this fraction is the less efficient the routing protocol. When the pause time is between 100 seconds to 300 seconds, Proposed secured routing protocol shows bigger normalized routing load than AODV; when it is between 300 seconds to 400 seconds, AODV shows bigger normalized routing load than proposed secured routing protocol and when pause time is between 400 seconds to 900 seconds, Proposed secured routing protocol shows marginal bigger normalized routing load than AODV. Although both the protocols give almost same results but still due to marginal difference between the results, we can

say that on an average AODV outperforms proposed secured routing protocol.

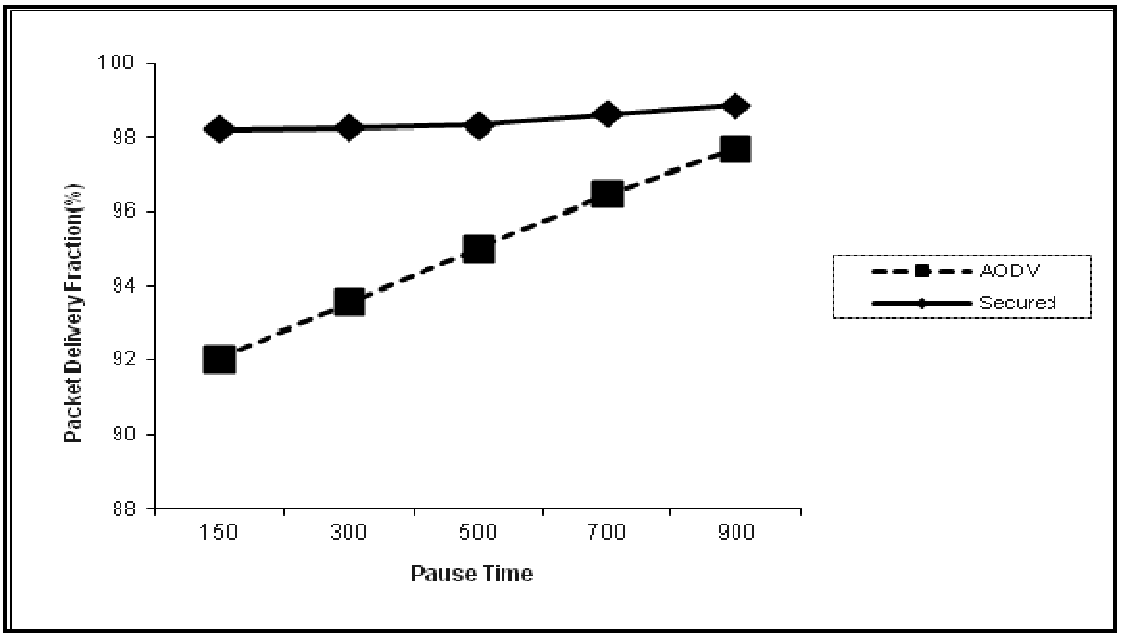

Figure 5. Packet Delivery Fraction

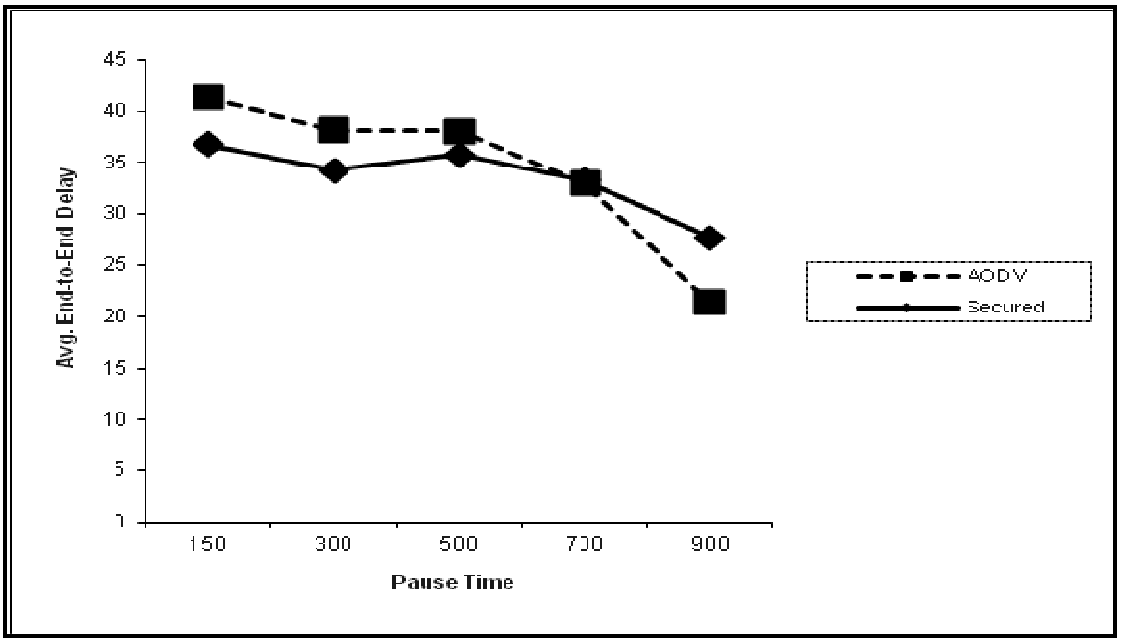

Figure 6. Average End to End Delay

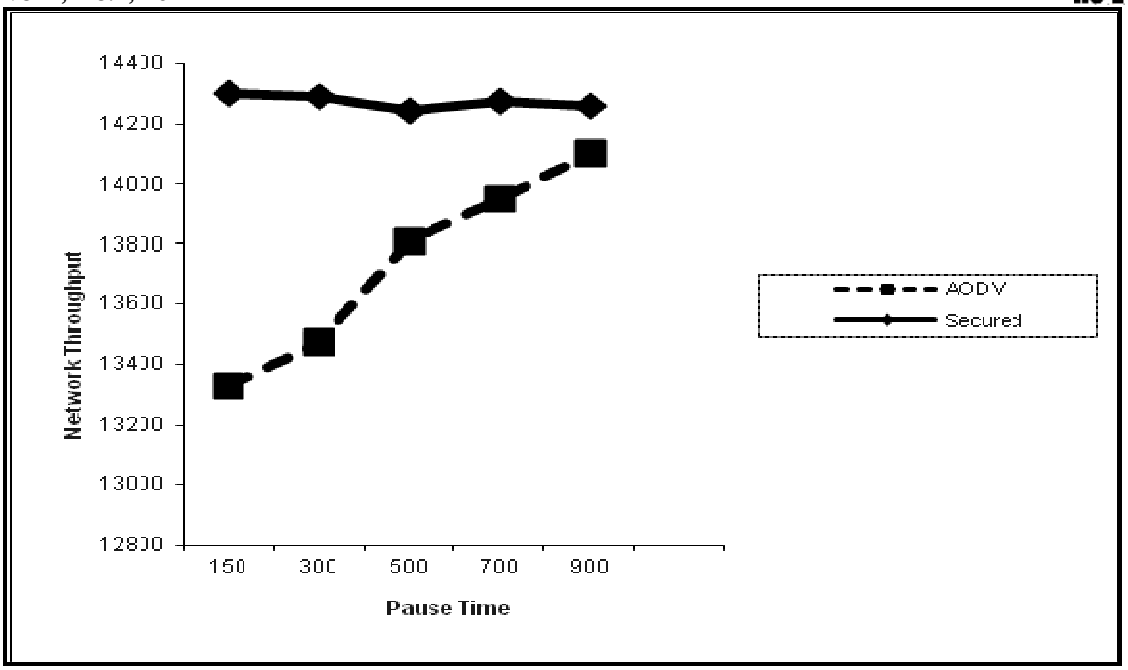

Figure 7. Network Throughput

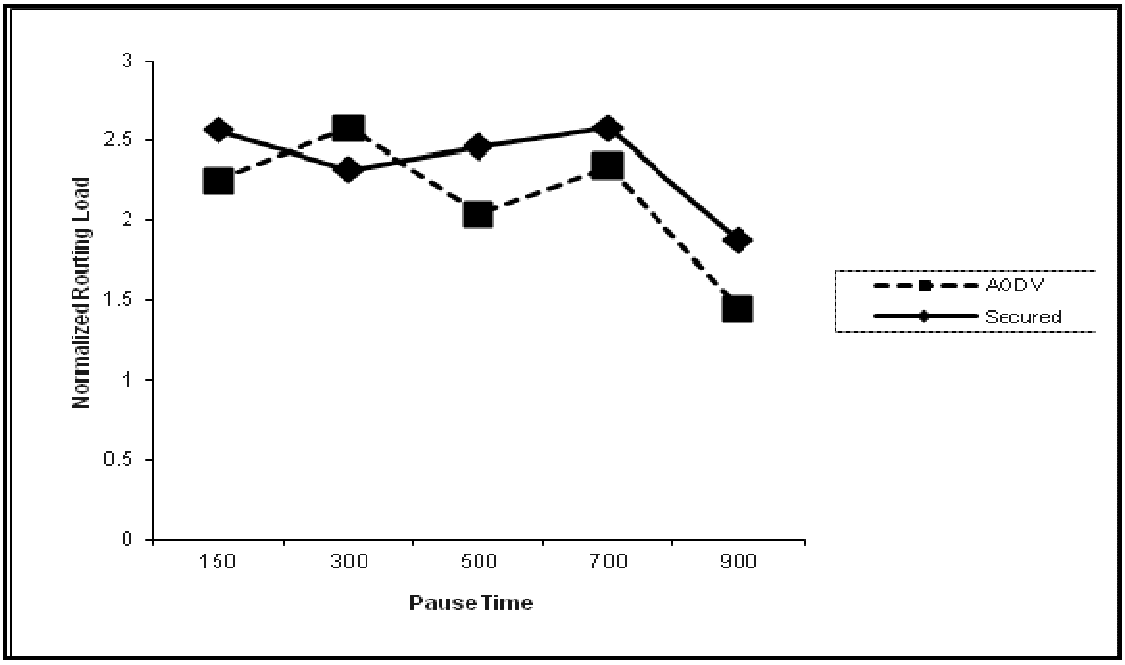

Figure 8. Normalized Routing Load

6. Conclusion and Future Scope

The existing MANET routing protocols normally follows the attack oriented design and implementation. Firstly, the various attacks on security are identified and then the existing protocol is enhanced to overcome the identified attacks. Since the protocol is enhanced by keeping in view the certain attacks, it may not handle the unexpected attacks on network security rather it provides secured routing in the presence of identified attacks only. Therefore, efforts have been done to propose a multifold and complete security solution for adhoc networking environment by developing a new on-demand secured routing protocol. The

proposed intrusion detection protocol tackles known and un-known security threats in a highly efficient manner by offering offers multiple lines of defense. The performance of proposed protocol has been evaluated with respect to AODV protocol using four primary quantitative metrics i.e. packet delivery fraction, average end to end delay, network throughput and normalized routing load. It has been concluded that when the malicious nodes come into the way over the adhoc networking environment, AODV protocol fails to handle the security threats but the proposed protocol conquer against the malicious attacks in a highly efficient manner. Efforts are in progress to increase the number of mobile nodes in the simulated model of adhoc networking environment and then to introduce more and more malicious nodes. Its impact on the performance of adhoc network needs to be determined by generating the appropriate network scenarios using network simulator. Efforts can also be done to enhance the hash functions and then to generate strong hash keys using some supplementary credential primitives like IP address, username, password and biometric etc.

References

Stallings, W. (2011), "Cryptography and Network Security: Principles and Practice", *Prentice Hall*, 5th Edition.

Dahill, B., Levine, B. N., Royer, E. & Shields, C. (2001), "A secure routing protocol for adhoc networks", *Technical Report UM-CS-2001-037*, University of Massachusetts, Department of Computer Science, 2001.

Papadimitratos, P. & Haas, Z. J. (2002), "Secure Routing for Mobile Adhoc Networks", *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, 2002.

Perrig, A., Johnson, D. B., Hu, Yih-Chun (2002), "ARIADNE: A Secure On-demand Routing Protocol for Adhoc Networks", *ACM, Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, 2002.

Zhou, L. & Haas, Z. J. (1999), "Securing Adhoc Networks", *IEEE Network Magazine*, 13(6), pp. 24–30, 1999.

Marti, S., Giuli, T. J., Lai, K. & Baker, M. (2000), "Mitigating Routing Misbehavior in Mobile Adhoc Networks", *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking*, pp. 255–265, 2000.

Arun, B. (2010), "Security in Adhoc Networks", Computer Science Department, University of Kentucky.

Johnson, D. B., Hu, Yih-Chun & Perrig A. (2002), "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Adhoc Networks," *IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pp. 3-13.

Zapata, M. G. & Asokan, N. (2002), "Securing Adhoc Routing Protocol", *WiSe*.

1 Partow, A. (2007), "General Purpose Hash Function Algorithms", www.partow.net, 2007.

Kush, A., Gupta, P. & Hwang C. (2009), "Secured Routing Scheme for Adhoc Networks", *International Journal of Computer Theory and Engineering (IJCTE)*, Volume 3. pp. 1793-1799.

Lamport, L. (1981), "Password Authentication with Insecure Communication", *Comm. of ACM*, 24 (11), pp. 770-772.