ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Comparison of Reactive Routing protocols in MANET using IDS system

K. Thamizhmaran
Department of Electronics and Communication Engineering,
Annamalai University, Annamalai Nagar,TN, India

Abstract: Mobile Ad-hoc networks (MANETs) is a infrastructure less network. They have so many advantages but disadvantages are security, transmission, energy etc. It has two types of protocols they are- reactive routing protocols and proactive routing protocols. In our paper, we discuss about comparing the security systems between the TORA (Temporally Ordered Routing Algorithm) and AODV (Ad-hoc on-demand distance vector routing) protocols using IDS (Intrusion Detection System) to get better result than proposed system. TORA is an algorithm for a routing data across MANETs, is an on-demand routing protocol. The main objective of TORA is to limit control message propagation in the highly dynamic mobile environment. AODV is an protocol establishes routes to destinations on demand and supports both unicast and multicast routing. The AODV protocol builds routes between nodes only if they are requested by source nodes. AODV creates a series of temporary nodes back to the requesting node. In our proposed system we compared parameters like Packet Delivery Ratio (PDR), Routing Overhead (RO) and Throughput through network simulation 2 (NS2).

Keywords- MANETs, IDS, protocols, TORA, AODV, security

1. INTRODUCTION

Compared with traditional networks, wireless mobile ad-hoc networks (MANETs) have fundamental characteristics of open medium, dynamic topology, lack of central authorities, distributed cooperation, and constrained capabilities. These characteristics present inherent vulnerabilities allowing malicious attackers to compromise the availability of the MANET or the integrity and confidentiality of the control and data traffic. Despite the best efforts of the protocol designers, implementers and network administrators, intrusion prevention measures such as authentication and encryption are not effective against all attacks, especially intrusions from insider or compromised nodes, a serious concern given the ease at which a mobile node may be physically compromised in a hostile environment. Therefore, it is vitally important to develop means to detect and respond to these attacks. If an intrusion is detected quickly enough, preventative and/or corrective measures can be employed to mitigate disruption or compromise. Towards that goal, this paper presents the results from design, implementation and evaluation of IDS to mitigate threats to routing in MANETs employing TORA and AODV.

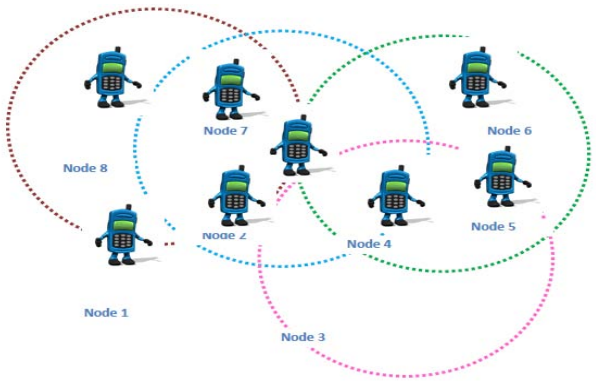

Fig 1 MANET

2. RELATED WORK

An IP-based quality of service framework for MANETs was done by Andrew T. Campbell et al (1999). Mitigating routing misbehavior in mobile ad-hoc networks was done by Marti et al (2000). Intrusion detection in wireless ad-hoc Networks was done by Zhang et al (2000). Routing security in wireless ad-hoc networks was done by Deng et al (2002). A Secure On-Demand Routing Protocol for ad-hoc networks Y.C.Hu et al (2002). Ad hoc On-Demand Distance Vector (AODV) Routing was done by Perkins et al (2003). Intrusion detection in MANETs – the second wall of defense was done by Ketan Nadkarni et al (2003). An advanced signature system for OLSR was done by Raffo et al (2004). Implementing a fully distributed certificate authority in an OLSR MANET was done by Dhillon et al (2004). An effective intrusion detection approach for OLSR MANET protocol was done by Wang *et al (2005)*. Bee ad-hoc: An Energy Efficient Routing Algorithm for Mobile Ad Hoc Networks Inspired by Bee Behavior was done by Horst f. wedde et al (2005). Perfect simulation and stationary of a class of mobility models was done by J.Y. Le Boudec et al (2005). Analysis of the node isolation attack against OLSR-based MANETs was done by Kannhavong et al (2006). Trust integrated cooperation architecture for MANETs was done by Balakrishnan et al (2007). Defense of trust management vulnerabilities in distributed networks was done by Y.Sun et al (2008). Performance analysis of MANET routing protocols in different mobility models was done by Jeya Kumar et al (2009). Performance analysis of AODV, DSR & TORA routing protocols was done by Anuj k. gupta et al (2010).

3. EXISTING SYSTEM

In previous paper, they used IDS cryptographic technique is used for OLSR (Optimized Link State Routing) routing protocol is only used. Being a proactive protocol, OLSR utilizes periodic messages to maintain topology information. The OLSR protocol is a variation of the classical Link State Routing (LSR) protocol designed specifically for MANETs.

The OLSR protocol achieves optimization over LSR through the use of Multipoint Relay (MPR) nodes that are selected amongst neighboring nodes. These optimizations limit the size and number of control traffic messages. They get high throughput and as well as get better results in IDS used OLSR protocol but their drawbacks are they doesn't used for other routing protocols. The proactive protocols are used in IDS secure system to get safer transmission purpose.

4. PROBLEM IDENTIFICATION

The existing system there problems are air interference and some routing protocols they didn't used IDS based system. In IDS based system, they didn't try to implement this system to other routing protocols and as well as didn't mention their which kind of attack their OLSR routing protocol.

5. PROPOSED SYSTEM

In our paper, if get a two reactive routing protocols just I used IDS in their two routing protocols. I compare the various parameters between the IDS based TORA and as well as AODV to get a better results in existing system. We have compared various parameters and getting better results IDS based AODV and TORA than OLSR. We see some conditions in my proposed system is given below.

5.1 DETECTING TC LINK SPOOFING-

Upon receiving a TC message initially from a node *Y* that lists itself, *X*, as a MPR selector, the recipient node *X* verifies that *Y* was first selected by *X* as a MPR.

Upon receiving a TC message that lists its neighbor *Y* as a MPR selector, a node *X* verifies that the message originates from a node which was selected by *Y* as a MPR in a Hello Message first.

Upon receiving a TC message originating from a neighbor *Y*, a node *X* verifies that the advertised MPR selector set is a subset of *Y*'s symmetric neighbor set, as advertised in *Y*'s Hello message.

5.2 DETECTING TC LINK AND MESSAGE WITHHOLDING-

A node *X* tests that within every TC_Interval seconds, a TC message is heard and processed from each node *Y* in its MPR set and that the TC message includes *X* as a MPR selector. If after TC_Interval seconds, TC messages have been processed but none of them contained *X*, it may indicate that node *Y* is withholding links.

In the case that no TC message is processed at all, it may judge that node Y is withholding TC messages.

To detect the special case of TC message withholding, nodes identify TC messages processed from their neighbor MPRs have a TTL value of 255.

5.3 DETECTING INCORRECT TC MESSAGE RELAYING-

Since TC messages are broadcasted, the sending node will overhear its MPRs relay the message further, allowing it to verify that protected fields are not tampered with.

If an entry remains in the record beyond a timeout period, it may indicate that the node is dropping TC messages.

6. SIMULATION ENVIRONMENT

The NS2 software is used to test the developed approach. Our simulation results with other research works, we adopted the default scenario settings in NS 2.34. In NS 2.34, the default configuration specifies 250 nodes in a flat space with a size of 700m× 700m. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. For every model, we ran every active network framework three moments and analysis the average performance. In order to analysis and compare the results of our developed scheme, we continue to adopt the following two performance metrics.

Table 1: Simulation Parameters

Parameter	values
Routing protocol	TORA, AODV
Application traffic	CBR
Transmission range	500m
Packet size	512 bytes
Transmission rate	6 packets/sec
Number of nodes	250
Area	700m*700m
Propagation model	Free space
Movement model	Random waypoint

7. RESULTS AND DISSCUSSION

In this technical research paper, detect the misbehaviour nodes when transmission and its provided secure communication from source to destination in this research work they simulate two different types on-demand routing protocols namely AODV and TORA, fixed topology, 250 nodes with different parameters PDR, RO, Throughput to simulate via network simulator 2.

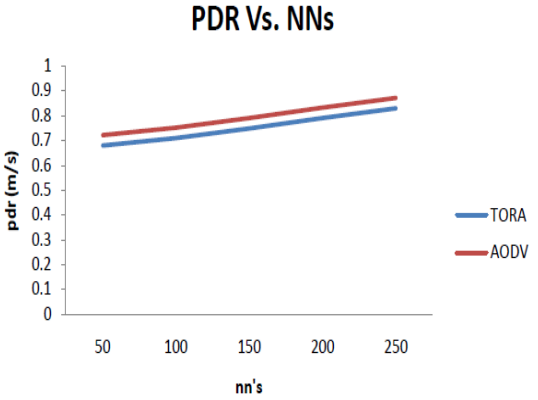

Fig 2 PDR Vs. NNs

Simulation outcomes of PDR are displayed in Fig 2 It is noted that AODV has the lowest overhead compared with TORA when there are 0 TO 250 nodes.

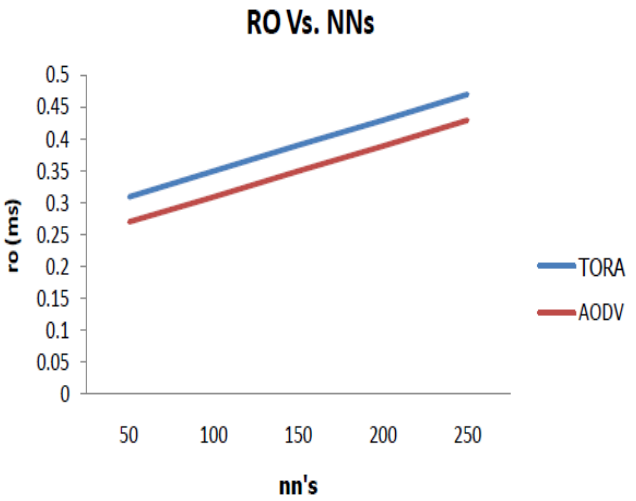

Fig 3 RO Vs. NNs

Simulation outcomes of RO are displayed in Fig 3 It is noted that AODV has the lowest overhead compared with TORA when there are 0 TO 250 nodes.

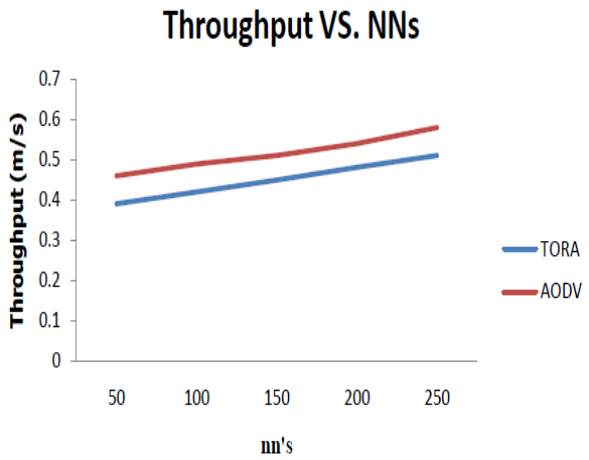

Fig 4 Throughput Vs. NNs

It is observed from Fig 4 that when compared with TORA on-demand routing protocol, AODV shows throughput improved with increase in the number of nodes.

8. CONCLUSION

In this proposed system, we get some better results than the IDS based OLSR. In future they get better results than mine. But I didn't specify any kind of attacks. In this research paper, a comprehensive TORA and AODV integrity threat analysis has been conducted and subsequently IDS, based on the analysis, is proposed. The IDS is implemented using a set of rules that locally check the integrity of TORA and AODV signaling messages and MPR behavior. The performance of the IDS is evaluated using ns-2 and quantified in terms of false positive and false negative detection rates in the presence of mobility. Simulation results indicate the presence of false positives that are positively correlated with mobility. Through the use of MPR history tables and delayed judgments, the frequency of false positives is demonstrably lowered, at the cost of false negatives for the rules involving message integrity checking. For other rules where false positives are difficult to eliminate due to message loss, a fundamental problem in wireless communication, we believe an environment adaptive threshold scheme may mitigate their effect. Future extensions of this work include an intrusion reaction mechanism for collaboratively accusing and isolating an intruder. As we compared various parameters concluded PDR, RO, Throughput to AODV is better than TORA.

9. REFERENCE

[1] Marti, et al (2000), "Mitigating routing misbehavior in mobile ad hoc networks".
[2] Zhang, et al (2000), "Intrusion detection in wireless ad hoc Networks".
[3] Deng, et al (2002), "Routing security in wireless ad hoc networks".
[4] Hu, et al (2002), "A Secure On-Demand Routing Protocol for Ad Hoc Networks".
[5] Perkins, et al (2003), "Ad hoc On-Demand Distance Vector (AODV) Routing".
[6] Ketan Nadkarni, et al (2003), "Intrusion detection in MANETs – the second wall of defense".
[7] Raffo, et al (2004), "An advanced signature system for OLSR".
[8] Dhillon, et al (2004), "Implementing a fully distributed certificate authority in an OLSR MANET".
[9] Wang, et al (2005), "An effective intrusion detection approach for OLSR MANET protocol".
[10] Le Boudec, et al (2005), "Perfect simulation and stationary of a class of mobility models".
[11] Kannhavong, et al (2006), "Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad-hoc Networks".
[12] Balakrishnan, et al (2007), "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks".
[13] Gupta, et al (2010), "Performance analysis of AODV, DSR & TORA routing protocols".
[14] Andrew, et al (1999), "INSIGNIA: An IP-Based Quality of Service Framework for Mobile Ad-hoc Networks".
[15] Horst, et al (2005), "Bee ad-hoc: An Energy Efficient Routing Algorithm for Mobile Ad-hoc Networks Inspired by Bee Behavior".
[16] Jeyakumar, et al (2009), "Performance analysis of MANET routing protocols in different mobility models".

AUTHOR'S PROFILE

K. Thamizhmaran has received his B.E and M.E degree from Annamalai University, Tamilnadu, India in the year of 2008 and 2012 respectively. He is currently working as an Assistant Professor in ECE, Department of Electronics and Communication Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamilnadu, India. He is a Reviewer of 03 International Journals. His research interested includes Networks security, Ad-hoc Networks, Mobile Communications. He has published more than 42 technical papers at various National / International Conferences and Journals. He is a member of IAENG, IACSIT.