ISSN : 2231-0711

A.R.Bharathidasan et al | International Journal of Computer Science Engineering and Technology(IJCSET) | Dec 2014 | Vol 4, Issue 12,349-352

Comparative Study on Spanning Tree Protocol and Trust Based Routing Protocol

A.R.Bharathidasan*[1], M.Yuvaraj*[2], G.Premnath*[3]

[1,2]*M.E Student,* [3]*Assistant Professor*

CSE DEPARTMENT, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College Chennai, Tamil Nadu

Abstract—A mobile ad-hoc network is a self-configuring network of mobile hosts connected by wireless links which together form an arbitrary topology. MANETs are finding ever-increasing applications in both military and civilian operations. Spanning Tree-enabled switches go through a root election process based on Bridge Protocol Data Unit (BPDU). All other switches then build the shortest, lowest-cost path to the root switch and block ports that are not along these shortest paths, resulting in a loop-free, tree-like topology. Without a protocol such as Spanning Tree, Layer 2 bridged networks are susceptible to broadcast/multicast and/or unknown unicast storms. Trust-Based Routing Protocol with controlled degree of Selfishness for Securing MANET against Packet Dropping Attack. It reduces the searching time of malicious nodes, and the routing protocol avoids the isolated misbehaving node from sharing in all future routes, which improves the overall network throughput. In his paper we are going to compare the study on spanning tree and trust based routing protocol. In this paper also do the performance analysis comparison.

Keywords— Mobile Ad Hoc Networks (MANETs), Spanning tree, Trust based routing

1.INTRODUCTION

Mobile Ad Hoc Network (MANET) is an infrastructure less network, consisting of a set of mobile nodes without any support of base stations or access points. MANETs are vulnerable to security threats due to the inherent characteristics of such networks, such as the open wireless medium and dynamic topology [8]. It is difficult to provide trusted and secure communications in adversarial environments, such as battlefields. It is clear that providing anonymity in ad hoc networks [4] is important as users may wish to hide the fact that they are accessing some service or communicating with another user.

In this paper we describe an anonymous on demand routing protocol for MANETs that is secure against both nodes that actively participate in the network and a passive global adversary that monitors all network traffic [6]. The high cost exacerbates the inherent resource constraint problem in MANETs especially in multimedia wireless applications.

Rapid development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment [5]. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing.

The privacy-preserving secure communication in hostile and suspicious MANETS. We construct a protocol for Anonymous Location-Aided Routing in MANETS (ALARM) [8] that demonstrates the feasibility of simultaneously obtaining, strong privacy, and security properties, with reasonable efficiency. While such MANET settings are not very common, they do occur in military and law enforcement domains and require high security and privacy guarantees. In this paper, we address a number of issues arising in suspicious location-based MANET settings by designing and analyzing a privacy-preserving and secure link-state based routing protocol.

2. SPANNING TREE

The Spanning Tree Protocol (STP) provides network link redundancy so that a Layer 2 switched network can recover from failures without intervention in a timely manner. The STP is defined in the IEEE 802.1D standard. This implementation guide will provide a basic understanding of all three versions of the Spanning Tree Protocol, namely 802.1d-1998, RSTP (802.1w) and MSTP (802.1s), as well as background on common enterprise networks and how to deploy EX Series switches in a mixed environment with Juniper Networks MX Series 3D Universal Edge Routers and Cisco switches.

2.1 SPANNING TREE PROTOCOL OVERVIEW

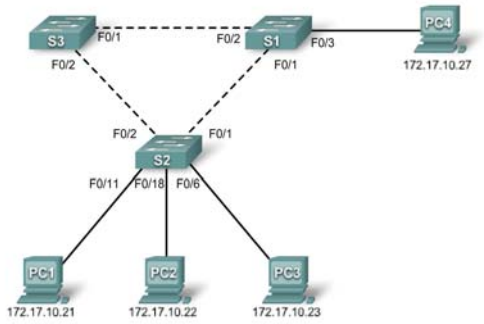
The plug-and-play Spanning Tree Protocol (STP), a Layer 2 protocol that ensures a loop-free topology in bridged LANs, has been around for decades. Spanning Tree-enabled switches go through a root election process based on Bridge Protocol Data Unit (BPDU). All other switches then build the shortest, lowest-cost path to the root switch and block ports that are not along these shortest paths, resulting in a loop-free, tree-like topology. Without a protocol such as Spanning Tree, Layer 2 bridged networks are susceptible to broadcast/multicast and/or unknown unicast storms. In the next few bullets, we will discuss three different versions of standards-based STP, and then talk briefly about Cisco's Spanning Tree implementation—Per-VLAN Spanning Tree Plus (PV ST+).

Spanning Tree Protocol (STP–802.1d 1998): The original version of STP (legacy STP) only supports a single instance of Spanning Tree in a bridged network, typically referred to as Common Spanning Tree (CST). On 802.1Q trunks that carry multiple VLANs, one VLAN—usually the

default or VLAN 1—will dictate the forwarding topology for all other VLANs. In STP, when a port is enabled or there is any change in the STP topology, it can take up to 50 seconds (MAX_Age + 2 x FWD_Delay, with default timers) for the bridged network to recon verge.

STP is communicated among all connected switches on a network. Each switch executes the Spanning Tree Algorithm based on information received from other neighboring switches. The algorithm chooses a reference point in the network and calculates all the redundant paths to that reference point. When redundant paths are found, the Spanning Tree Algorithm picks one path by which to forward frames and disables, or blocks, forwarding on the other redundant paths.

2.2 Basic Spanning Tree Protocol



Topology diagram

2.3 STP States

To participate in STP, each port of a switch must progress through several states. A port begins its life in a Disabled state, moving through several passive states and, finally, into an active state if allowed to forward traffic. The STP port states are as follows:

- **Disabled**—Ports that are administratively shut down by the network administrator, or by the system because of a fault condition, are in the Disabled state. This state is special and is not part of the normal STP progression for a port.
- **Blocking**—After a port initializes, it begins in the Blocking state so that no bridging loops can form. In the Blocking state, a port cannot receive or transmit data and cannot add MAC addresses to its address table. Instead, a port is allowed to receive only BPDUs so that the switch can hear from other neighboring switches. In addition, ports that are put into standby mode to remove a bridging loop enter the Blocking state.
- **Listening**—A port is moved from Blocking to Listening if the switch thinks that the port can be selected as a Root Port or Designated Port. In other words, the port is on its way to begin forwarding traffic. In the Listening state, the port still cannot send or receive data frames. However, the port is allowed to receive and send BPDUs so that it actively can participate in the Spanning Tree topology process. Here, the port finally is allowed to become a Root Port or Designated Port because the switch can advertise the port by sending BPDUs to other switches. If the port loses its Root Port or Designated Port status, it returns to the Blocking state.
- **Learning**—After a period of time called the Forward Delay in the Listening state, the port is allowed to move into the Learning state. The port still sends and receives BPDUs as before. In addition, the switch now can learn new MAC addresses to add to its address table. This gives the port an extra period of silent participation and allows the switch to assemble at least some address table information. The port cannot yet send any data frames, however.
- **Forwarding**—After another Forward Delay period of time in the Learning state, the port is allowed to move into the Forwarding state. The port now can send and receive data frames, collect MAC addresses in its address table, and send and receive BPDUs. The port is now a fully functioning switch port within the spanning-tree topology.

3. TRUST BASED ROUTING PROTOCOL

Trust-Based Routing Protocol with controlled degree of Selfishness for Securing MANET against Packet Dropping Attack [3].TMR provides a method of message security using trust based multipath routing. In this approach, less trusted nodes are given lesser number of self encrypted parts of a message, thereby making it difficult for malicious nodes to gain access to the minimum information required to break through the encryption strategy [4]. Using trust levels, it makes multipath routing flexible enough to be usable in networks with “vital” nodes and absence of necessary redundancy. In addition, using trust levels, it avoids the non trusted nodes in the routes that may use brute force attacks and may decrypt messages if enough parts of the message are available to them.

The trust routing protocols have to be able to identify trustworthy nodes and find a reliable and trustworthy route from sender to destination node. This has to be realized within a few seconds or better tenths of seconds, depending on the mobility of the nodes and the number of hops in the route.

The secure routing in ad hoc networks as discussed in the earlier section is based on key management or heavy encryption techniques or on continuous promiscuous monitoring of the neighbors. The trust based routing which protects the message against modification [2]. In this, trust is calculated in a dynamic way and less trusted path may also be used to transmit data depending upon the security requirement of the message. It makes use of an encryption technique not requiring intensive computations [1]. Before selecting the final paths, source waits for RREP from different paths and if all the paths have trust less than the required trust, the message is divided, encrypted and then sent. This increases the delay in routing.

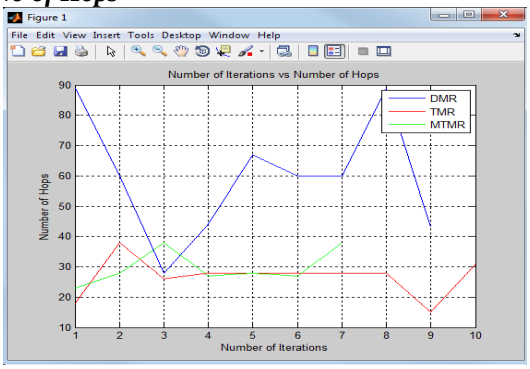
The three routing algorithms are presented namely disjoint multipath routing (DMR), Trust based multipath routing (TMR), and message trust based multipath routing (MTMR)[4]. All the three routing protocols have their own

way in order to establish the trust and transmit packet securely. The performance metric considered are, number of hops, route discovery time and packet loss, The simulation results show that MTMR protocol works much better and provides less number of hops, less route discovery time and less packet loss.

Trusted Dynamic Source Routing (TDSR) extends the widely used DSR routing protocol and employs the idea of Trust Network Connect (TNC) to protect routing behaviors. In the TDSR, trust among nodes is represented by trust score, which consists of direct trust and indirect trust.

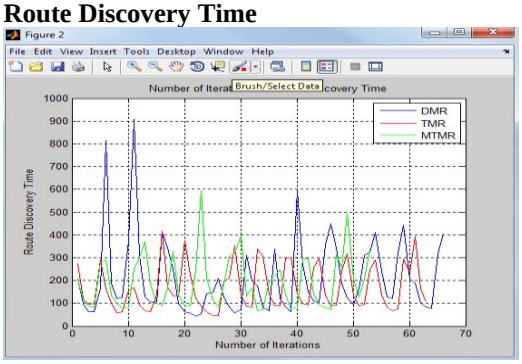
3.1 PERFORMANCE ANALYSIS OF ALGORITHMS

1. No of Hops



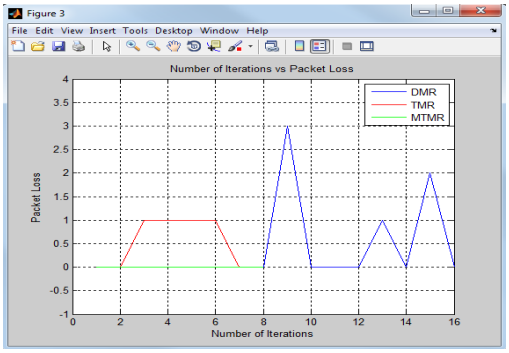
The number of hops taken from source to destination for all three algorithms. It is observed from the graph that the number of hops for the MTMR algorithm is least.

2. Route Discovery Time



The route discovery time taken from source to destination for all the three algorithms. It is observed from the graph that the route discovery time for the MTMR algorithm is least.

3. Packet Loss



The packet taken from source to destination for all three algorithms. DMR is having a more number of packet losses. Packet drop is minimal and almost zero in MTMR algorithm, as it will detect more malicious nodes.

But other multipath routing protocols drop a larger number of packets as they route through a greater number of nodes and thus increasing the chances of routing data through malicious nodes.

It is observed from the figure that the packet loss for the MTMR algorithm is nil or zero.

4. ALGORITHM DETAILS:

AES (Asymmetric Encryption Standard):

This algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14). These rounds are governed by the following transformations.

(i) **Byte Substitution**: This is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation.

(ii) **Shifting the rows**: This is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.

(iii) **Mixing of columns**: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

(iv) **Adding round key**: Is a simple XOR between the working state and the round key. This transformation is its own inverse.

5. CONCLUSION

In this paper a new approach is used as trust based routing protocol will provide the encryption of cryptosystem to provide more security for data owner whose who upload the data and data user efficiently will reduce the packet delay from the analysis results shown above. Also provide the security for packet transmission in Manet, performance calculated and results are analyzed.

ACKNOWLEDGMENT

I would like to thank my guide Mr.G.Premnath for assisting me in this paper work.

REFERENCES

[1] Mohana [1], N.K. Srinath [2], Amit L.K3, "Trust Based Routing Algorithms for Mobile Ad-hoc Network", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012)

[2] Ahmed M. Abd El-Haleem [1] and Ihab A. **Ali** [2], "TRIUMF: Trust-Based Routing Protocol with controlled degree of Selfishness for Securing MANET against Packet Dropping Attack", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011 ISSN (Online).

[3] Deepak Kukreja, Umang Singh, and B. V. R. Reddy, "A Survey of Trust Based Routing Protocols in MANETs", *Journal of Advances in Computer Networks, Vol. 1, No. 4, December 2013.*

[4] Jiejun Kong, Xiaoyan Hong, and Mario Gerla, "An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc, Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 8, AUGUST 2007.

[5] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang,"MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 5, NO. 9, SEPTEMBER 2006.

[6] Michael G. Reed, Paul F. Syverson, and David M. Goldschlag,"Anonymous Connections and Onion Routing", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 16, NO. 4, MAY 1998.

[7] Xiaoqing Li, Hui Li, Jianfeng Ma, Weidong Zhang,"An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks", 2009 Fifth International Conference on Information Assurance and Security.

[8] Karim El Defrawy, and Gene Tsudik," Privacy-Preserving Location-Based On-DemandRouting in MANETs", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 10, DECEMBER 2011.