International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com‖ Volume 2 Issue 1‖ January 2016 ‖ PP 16-22

MULTI PATTERN AND REPUTATION BASED SECURITY IN MANET

Sheetal Jaiswal
Department Of Computer Science & Engineering
S.D.Bansal College Of Technology,Indore, India

Shraddha Kumar
Department Of Computer Science & Engineering
S.D.Bansal College Of Technology, Indore, India

Abstract- Various routing protocols and techniques are being included in wireless network and making it an area for further research. Congestion avoidance and security are the major areas in Wireless routing which are having research focus. Improved Routing Security is being proposed in this work which will provide the routing protocol security using validating a node for identification which is being distributed to each node through protocol.. Various researchers have identified the issues related with it and proposed various mechanism to solve this problem. This work proposes a new algorithm based on reputation and key based security for the MANET to improve the security. The basic algorithm is based on reputation value of the communicating node i.e. it should be comparable with each other for accepting nodes in the network. Once reputation is found to be comparable node exchange the keys for further communication.
Keywords— MANET, Reputation, Multi pattern Key, DSDV.

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are technically different from the traditional wireless networks (e.g. wireless LANs, cellular, digital trunked radio or satellite networks). In traditional wireless networks, the fixed network infrastructures such as access points, base stations or satellites are necessarily required to function as the repeaters to relay/retransmit the signal from one node to the others. However, none of these network infrastructures is required in ad hoc networks that are why ad hoc networks are sometimes called as infrastructure less wireless networks.

This paper provides a modified trust mechanism for increasing the security over MANET using IBC along with reduced processing time and load on the system. It assigns keys to every incoming node which is used only once per communication between the nodes and hence high performance is assured[1]

Security in mobile ad-hoc networks (MANETs) continues to attract attention after years of research. Recent advances in identity-based cryptography (IBC) sheds light on this problem and has become popular as a solution base. We present a comprehensive picture and capture the state of the art of IBC security applications in MANETs based on a survey of publications on this topic since the emergence of IBC in 2001. In this paper, we also share insights into open research problems and point out interesting future directions in this area. [2]

Nowadays, security is on highest priority since MANETs are being deployed in hostile environments. For achieving security, required services include authentication, confidentiality, integrity, availability, and non repudiation.

Security measures applied in wired networks are not applicable to MANETs as the characteristics of wireless networks are different due to their "open" network architecture, shared wireless medium, resource constraints, and dynamic network topology impose restrictions for MANETs.[3]

In MANET there are various problems due to its open architecture such as access of the wireless channel is available to the eavesdroppers, malicious attackers, legitimate users, hackers etc. Also, there can be defined nodes which will monitor the network traffic or where access control methods can be deployed means there is no clear line of defense can be drawn. Each MANET node functions as router and forwards packets to other peer nodes. Traditional fixed wired networks have dedicated infrastructure such as firewalls, routers, and Intrusion Detection Systems (IDS) to provide protection from outside threats. We can define the difference between the "inside" and "outside" network which may be the way for adding security in the network. Trusted environment is therefore applied by the routing protocols over MANETs, as there is no clear threat to defend against. [4]

This paper presents a holistic security framework called Reputation-based Internet Security (RIPsec) that leverages existing technologies to provide a more comprehensive security solution. This includes a combination of behavior grading, link and message encryption and multipath routing. The main contribution of this framework is a methodology that provides a MANET capable of supporting high bandwidth applications (e.g., video and imagery) protected from both internal and external threats.[5]

The growth of laptops and 802.11 / Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

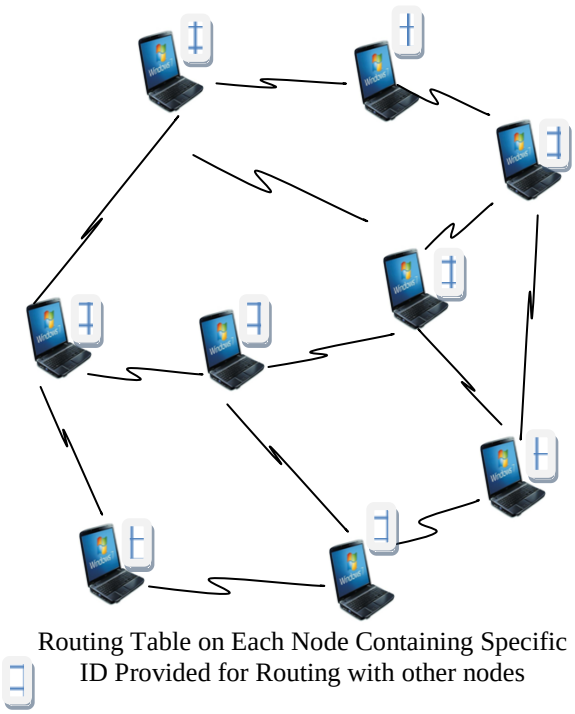

Figure 1: Shows the Network Topology for MANET

Ad Hoc Routing Protocols are classified into Proactive and Reactive type. Proactive routing protocols use the periodic update of information to know about the current topology while the reactive routing protocols create a route to a destination on demand basis. Few of the proactive protocols are Distribution-Sequence Distance-Vector Routing (DSDV) [11] [12], Wireless Routing Protocol (WRP) [12] [14], and Distributed Bellman-Ford (DBF) etc. while Dynamic Source Routing (DSR) [15], Ad hoc On-Demand Distance Vector (AODV) Routing [13], and ABR are few examples of reactive protocols. Even though no protocol is superior to the other, but the previous studies indicate that in general reactive protocols exhibit better performance than proactive protocols.

II. EXISTING SYSTEM

MANETs is a collection of wireless nodes which will dynamically kind a network to exchange data while not using any pre-existing fixed network infrastructure with or while not centralized network controller. Mobile ad-hoc Networks are getting useful due to the existing wireless infrastructure is costly and not convenient currently days. Mobile Ad-Hoc Networks is becoming important part of next generation mobile services.
From the higher than discussion it's been found that several researchers have already worked within the area of wireless security and research remains occurring.

Research within the area can be divided into two groups:

- Security in Routing Protocols and applications i.e. mechanism security
- Security of data being transferred over the network.

Work of the various researchers is focusing on trust based security and key management. Where the key is obtained from the trust server and then it is authenticated on every node by the trust server.
The limitation of above work is that day takes extra authentication time result is reduce throughput. This affects the network performance drastically.
Some of the authors have worked on local key management but it is limited to only one key being generated locally and if malicious user compromise key pattern then it may be security threat [1].
Researcher focuses on pattern key distribution among the nodes which are communicating with each other and carry the sufficient risk of leak of pattern and affecting the communication severely.
Trust management, though are self addressed totally still new problem are occurring and causing the topic to be addressed once again.
Major points to be addressed are:

- Impact of Heterogeneous Nodes on trust
- Security Paradigm to enhance trust within the network
- Social and context dependent trust.

Impact of heterogeneous nodes on trust: Heterogeneity implies that not all nodes or their contents can be treated equally once it involves to trust evaluations. Thus, the same functional descriptions will not be applied to evaluate the trust levels of all nodes and their information [16].

Impact of network dynamics on trust: Mobility will impact the trust propagations and varied different security paradigms. Similarly, the connection between different network dynamics (including link dynamics, network density) and trust and its dynamics however to be analyzed [17].

III. PROPOSED WORK

In MANET, various nodes come nearby to each other and form a network and therefore security is a primary issue in such networks. Security is to be considered for

- Routing Protocol Security
- Data Security

The proposed algorithm has following building block mechanisms characteristics:

1. It adds malicious nodes at the time of creation of the topology for each node by randomly selecting some of the nodes to be malicious. It will also add an initial reputation and will also generate a pattern key for each node.
2. Frames of Ready To Send (RTS) are added which will carry the reputation and key of the sender node to the receiver node. Reputation is used to include the node in network which leads for pattern key authentication of the nodes before actual communication starts.
3. Each node will first send the reputation and key to descendant node, which will be verified for the specific pattern. If the reputation is found to be comparable and key is successfully verified then the node sends the CTS signal to sender. The sender will get the key of receiver and will authenticate it. This, two way verification process, incorporates the security of the nodes before actual transfer of the data.

Steps in the proposed algorithm are as follows:
Step 1: The algorithm will start by creating a topology.
Step 2: Each node will be initialized with an initial reputation (R) value of zero.
Step 3: When any node will start sending data to another node then the second node will increase the reputation by a factor R1.
Step 4: Any node will be allowed to communicate with another node if the reputation of the nodes must not differ by a reputation +/- threshold value (0.5).
Step 5: The security incorporated will only allow the nodes with similar reputation in the network therefore any newly entering malicious node will not be able to communicate with existing nodes which are having a higher reputation.
Step 6: Higher reputation will indicate that node is involved in lot of communication and hence it is an important node.
Step 7: Each node is provided with a fixed and random pattern of the public key for communication over the network, which shall be generated at the time of the creation of the node.
The key will be generated using a Pseudo Random Generator, which is not only generating Random Keys but will also generate keys in Random Pattern for each node.

Step 8: When one node wants to communicate with another node in the topology, then it will read the best route from the routing table of the DSDV.
Step 9: The sender node will verify the keys available on each node whether they are similar or not in the best route.
Step 10: If the keys on one or more nodes are not matching then the best route will not be used by the sender and it will look for alternate path for data transfer. The alternate path is also checked for security.
Step 11: If the keys are matched properly for the specified path then it will be used for transferring data.
Step 12: The algorithm will be eliminate the crucial safe information and it's also provide a secure route for communication over the network.
Security of the network is being checked by using NetworkSimulator-2 simulation environment. The throughput of the network along with end to end delay has been calculated for packet sizes 256 Bytes. The simulation has been performed using 5, 10, 15, 20, 25, 30, 35, 40, 45, and 50 nodes.

IV. IMPLEMENTATION

A. SIMULATION ENVIRONMENT

NS-2.32 could be a discrete event simulation tool of network nodes whenever the time depends on the simulation event and that are maintained by user. It supports two languages: first is object oriented simulator written in c++ language and second is object oriented tool command language (OTcl) interpreter for execution of the user's command script. In NS object oriented simulator providing fast simulation from slow to changes of code, it's appropriate for detailed protocol implementation and OTcl provides that a lot of slower simulation however user will be modified easily, it's primarily based for network configuration. The compiled c++ hierarchy allows as achieving efficiency in the simulation and faster execution times and within the OTcl script we will define the particular network topology, specific protocol and application that we would like to simulate and type of the object that we wish to get from the simulation.

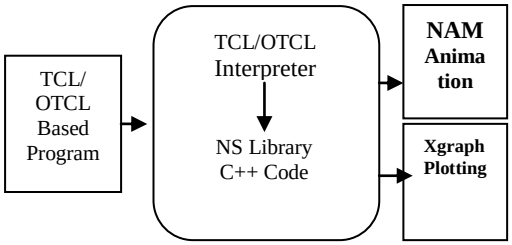

Figure 2: NS-2 Architecture

B. SIMULATION PARAMETERS

Channel	Channel /Wireless Channel
Propagation	Propagation /Two Ray Ground
Network Interface	Phy/ Wireless Phy
MAC Protocol	Mac/802_11
Interface Queue	Queue/Drop Tail/PriQueue
Link Layer Type	LL
Antenna	Antenna/Omni Antenna
Queue Size	50
Routing Protocol	DSDV
Topology Area Width	670 Square Feet
Topology Area Height	670 Square Feet
Maximum Time	3 Seconds
Bandwidth	100 Mbps
Link Delay	10 ms Drop Tail
Traffic Generator	CBR

packet sizes	256 bytes.
Number of Mobile Nodes	5- 50

The simulation parameters used are shown in table 1.

V. SIMULATION RESULTS

The animation behavior is indicative of the success of the proposed work. Simulation has been performed for the traditional IEEE 802.11 protocol with inclusion of malicious nodes and once applying the proposed security model with malicious nodes. Malicious nodes are enclosed by creating changes within the default implementation of 802.11 headers without key and rest of the nodes is given a pattern key. The key is used as in the proposed work

Throughput, PDR, ETOE Delay can be calculated for each and therefore the graphs are drawn using XGRAPH utility of the Linux. Simulation has been performed packet sizes 256 Bytes. The graph of 256 Bytes for throughput Packet Delivery Ratio and end to end delay

1. Throughput

The graph in Figure shown that the Throughput is better in all scenarios of the number of nodes expect in scenario 20 nodes and the reason for the same can be due to random topology of the node create for simulation.

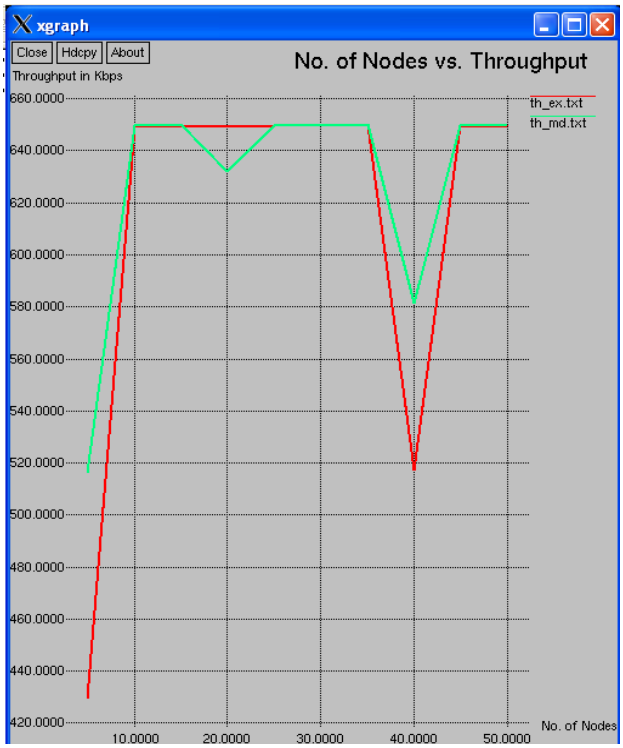

Figure 3: Throughput comparison graph in Network

2. Packet Delivery ratios

From the graph, it's seen that the values of the PDR for proposed implementation are higher than the values of PDR of existing work and it's concluded that the performance of the proposed implementation is more than the other existing routing protocols. High PDR means that the numbers of packets being sent are reaching to the destination in more count and also the loss of packets in manner the less and this will increases reliability for any network. The reason for the similar due to the use of reputation algorithm which uses reputation value to decide the route by that the packets can traverse to the destination. This mechanism of route decision is most reliable and will not overload any route whenever congestion will occur.

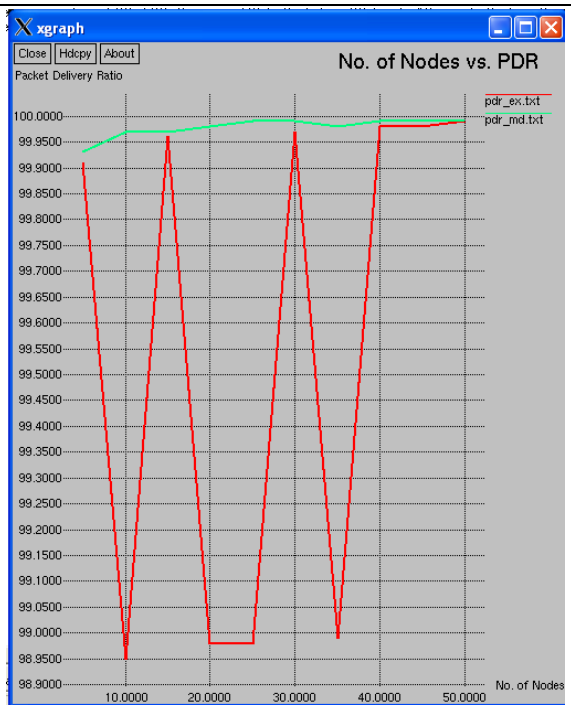

Figure 4: Packet Delivery Ratio comparison graph in Network

3. End To End Delay

From the graph, it's seen that the values of the Average Delay for proposed implementation are less than the values of Average Delay of other graphs and it's concluded that all over the performance of the proposed implementation is higher than the other existing routing protocols in terms of time taken by any packet to reach to destination. Low average delay means numbers of packets being sent are reaching to the destination. This can be occurring because the throughout is high so network delays are very less and packets on not stopping in congestion on the nodes or the networks. DSDV has higher average delays because the route calculation time is decreased in it.

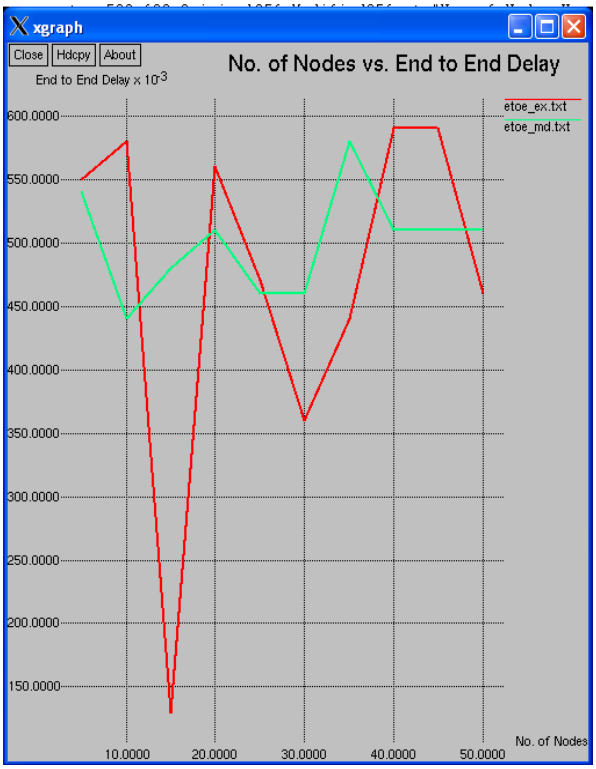

Figure 5: End To End Delays Comparison Graph in Network

VI. CONCLUSION

In MANET major problems are identified to be of congestion and security. Out of those security is major problem as with the growth of the technology speed of networks is increasing very fast.

This research focus on providing a security algorithm that may dynamically adjust the route formation and avoid the formation of less reliable route. More reliable route formation is helpful in providing reliable services in Mobile Ad-Hoc Networks. Our approach also decreases the result of the packet loss rate among the nodes. It also helps to get best route with minimum value to maximize the Packet Delivery Ratio and minimize routing overhead and therefore the average end-to-end delay.

Node having the higher reputation value is selected as a next hop. Node's reputation is depending on the attitude of the node to forward the packets further in place of dropping them as the malicious nodes do. These values are changing with the random movement of nodes. We have gone through extensive simulation using ns2 simulator.

The implemented work can be tested for high density of nodes having wireless nodes. The high density networks shall cause the more chances of having higher amount of traffic and more chances of malicious nodes in the network hence the working of the proposed work shall be checked up to great extent.

In future, Reputation threshold has been fixed and manually decided in the current work. This can be made dynamic using different parameters such as amount of traffic forward by a node or available bandwidth and this work can also be enhanced to test on other protocols such as AODV or DSR.

REFERENCES

[1]. Agrawal, R.; Sahu, S., "Secured routing over manet using Enhanced Secured Routing (ESR)," Control Computing Communication & Materials (ICCCCM), 2013 International Conference on , vol., no., pp.1,6, 3-4 Aug. 2013.

[2]. Shushan Zhao, Akshai Aggarwal, Richard Frost and Xiaole Bai, "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks," IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, Second Quarter 2012.

[3]. Salaheddin Darwish, Simon J. E. Taylor and Gheorghita Ghinea, "Security Server-Based Architecture for Mobile Ad hoc Networks," IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 978-0-7695-4745-9, 2012.

[4]. Erman Ayday and Faramarz Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 9, SEPTEMBER 2012, 1536-1233, SECOND QUARTER2012.

[5]. S.Neelavathy Pari, Sabarish Jayapal and Sridharan Duraisamy "A Trust System In Manet With Secure Key Authentication Mechanism," IEEE, ISBN: 978-1-4673-1601-9, 2012.

[6]. L. Abusalah, A. Khokhar and M. Guizani, "A survey of secure mobile ad hoc routing protocols," IEEE Commun. Surveys & Tutorials, IEEE, vol. 10, no. 4, pp. 78–93, 2008.

[7]. A.Shamir, "Identity-based cryptosystems and signatureschemes," Proc. Crypto 1984, 1984.

[8]. J. Marc and N. Gregory, "Identity-Based Cryptography," IOS Press, ISBN 978-1-58603-947-9, 2009.

[9]. Yang H and Meng X, Lu S, "Self-organized network-layer security in mobile ad hoc networks," 1st ACM Workshop on wireless security, ACM; PP. 20, 2002.

[10]. Hu YC, Jognson DB and Perrig A, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," Ad Hoc Network, pp 175-92, 2003.

[11]. S. Corson and J. Macker, "Mobile AdHoc Networking (MANET): Routing Protocol Performance issues and Evaluation Considerations", Network Working Group, RFC2501, January 1999

[12]. Khaleel Ur Rahman Khan, A Venugopal Reddy, Rafi U Zaman, K. Aditya Reddy, T Sri Harsha "An Efficient DSDV Routing Protocol for Wireless Mobile Ad Hoc Networks and its Performance Comparison", IEEE 978-0-7695-3325-4/08, Second UKSIM European Symposium on Computer Modeling and Simulation, 2008

[13]. Y. Su and T. Gross, "WXCP: Explicit congestion control for wireless multi-hop networks," in Proc. of IWQoS, Jun. 2005

[14]. A.Kowshika, C.Maheswari, Dr.S.Karthik. "A Packet Forwarding Mechanism for MANET using MODRP in Dynamic Source Routing (DSR)," 2010 International Conference on Advances in Recent Technologies in Communication and Computing

[15]. Wireless Data Networking Standards Support Report: 802.11 Wireless Networking Standards, 2002

[16]. Shushan Zhao, Akshai Aggarwal, Richard Frost, Xiaole Bai, "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks", IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, Second Quarter 2012 1553-877x (C) 2012 IEEE

[17]. Salaheddin Darwish, Simon J. E. Taylor and Gheorghita Ghinea, "Security Server-Based Architecture for Mobile Ad hoc Networks", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications 978-0-7695-4745-9 © 2012 IEEE OI 10.1109/TrustCom.2012.260