EFFICIENT SECURE TOPOLOGY CONTROL PROTOCOL FOR AUTHENTICATION IN MANET

[1]T.S.ASHA, [2] DR.N.J.R.MUNIRAJ
[1] Research Scholar, Karpagam University, Coimbatore, India
[2]Principal, Tejaa Shakthi Institute of Technology, Coimbatore
E-mail: tsasha_tcs@gmail.com

ABSTRACT

Mobile Ad hoc Network consists of mobile nodes without any access point. Due to that, nodes are easily compromised by means of attackers. Attackers totally degrade the performance of network. Several researches focused the solution for security issues. In this research work, we propose Efficient Secure Topology Control Protocol (ESTCP) to make the balance between interference and security in order to improve the reliability of networks. It consists of four phases In first phase, we propose the efficient topology control approach which consists of minimal weight estimation and exchanging information, topology estimation. In second phase, Cluster is formed and cluster head is chosen. In third phase, multipath is deployed to improve reliability. In fourth phase, messages are encrypted and decrypted using RS codeword. By using the extensive simulation results using Network Simulator (NS3), the proposed scheme NCTC achieves better network lifetime, packet delivery ratio, less overhead and end to end delay than the existing schemes.

Keywords: *MANET, Interference, multipath routing, secure encryption and decryption, cluster formation, network connectivity, network lifetime, packet delivery ratio, end to end delay, overhead.*

1. INTRODUCTION

1.1 Mobile Ad Hoc Networks (MANET)

Mobile ad-hoc network is an independent system of mobile nodes connected by wireless links forming a short, live, on-the-fly network even when access to the Internet is unavailable. Nodes in MANETs generally operate on low power battery devices. These nodes can function both as hosts and as routers. As a host, nodes function as a source and destination in the network and as a router, nodes act as intermediate bridges between the source and the destination giving store-and-forward services to all the neighbouring nodes in the network. Easy deployment, speed of development, and decreased dependency on the infrastructure is the main reasons to use ad-hoc network.

1.2 The topology control issue in MANET

In mobile ad hoc wireless communication, each node of the network has a potential of varying the topology through the adjustment of its power transmission in relation to other nodes in the neighborhood. In contrast, wired networks have fixed established pre-configured infrastructure with centralized network management system structure in place. Therefore, the fundamental reason for the topology control scheme in MANET is to provide a control mechanism that maintains the network connectivity and performance optimization by prolonging network lifetime and maximizing network throughput. A MANET topology can depend on uncontrollable factors such as node mobility, weather, interference, noise as well as controllable factors such as transmission power, directional antennas and multi-channel communications. A bad topology can impact negatively on the network capacity by limiting spatial reuse capability of the communication channel and also can greatly undermine the robustness of the network. Network capacity means the bandwidth and ability for it to be used for communication. A network partitioning can occur in a situation where the network topology becomes too sparse. Similarly, a network which is too dense is prone to interference at the medium access (MAC) layer, the physical layer of the network. So the network should neither be too dense nor too sparse for efficient communication amongst nodes to take place.

1.3 *Security goals and threats*

Ideally, one would like the network security to degrade gracefully with the number of compromised nodes. We consider three types of attack and assume that some link-level security mechanism is implemented to protect the network against these attacks in the absence of node compromise.

- **Eavesdropping:** Eavesdropping occurs when an attacker compromises an aggregator node and listens to the traffic that goes through it without altering its behavior. Since an aggregator node processes various pieces of data from several nodes in the network, it does not only leak information about a specific compromised node, but from a group of nodes.
- ***Data tampering and packet injection***: A compromised node may alter packets that go through it. It may also inject false messages. Since an aggregate message embeds information from several sensor nodes, it is more interesting for an attacker to tamper with such messages than simple sensor readings. An attacker that controls the meaning of the malicious messages it sends may heavily impact the final result computed by the sink.
- **Denial of Service:** A compromised node may stop aggregating and forwarding data. Doing so, it prevents the data sink from getting information from several nodes in the network. If the node still exchanges routing messages despite its unfair behavior, that problem may be difficult to solve. Smarter attacks also involve dropping messages randomly. It is also difficult to detect when an attacker sends garbage messages.

1.4 Problem Definition

The problem is identified in contemporary research literature pertaining to topology control in MANET is that most of the topology control algorithms do not achieve integrity, reliable and guaranteed network connectivity.

2. RELATED WORK

In this paper [1], Secure Link State Routing Protocol (SLSP) is proposed that provides secure proactive topology discovery. It can be employed as a stand-alone protocol, or fit naturally into a hybrid routing framework, when combined with a reactive protocol. It is robust against individual attackers and capable of adjusting its scope between local and network-wide topology discovery, and it is capable of operating in networks of frequently changing topology and membership.

In this paper [2], common possible attacks are addressed on different protocols being used in MANETs. Moreover, it was tried to analyze them so as to prevent the attacker to intrude in wireless networks. There are lots of techniques with which, one can easily detect most of the attacks. However, no protocol is fully secure from attacks being encountered in the MANETs.

In this paper [3], it is introduced that adopted authentication approach for protecting our Ad-hoc wireless network by even- odd function. Here, mobile node will compute and generates random even or odd number during signaling process. If first node generates random odd number then next node will do computation and generates random even number by incrementing of decrementing digit numbers. There are number of attacks existing in wireless communication in different application of communication field. This scheme provides more secure against all attacks.

In this paper [4], the problem of how record data path topology information is addressed in an efficient manner. It is explored that several mechanisms for efficiently recording this information and exchange it securely between nodes.

In this paper [5], a joint authentication and topology control (JATC) scheme is proposed to improve the throughput where the authentication is done in the upper layer and the channel conditions are given in the physical layer. Transmission reliability is improved by the cooperation communication. It was addressed that no cooperation and multipath routing is established between mobile nodes in previous work.

In this paper [6], it was tried to explain the protocols protected route discovery from malicious nodes in both reactive and proactive topologies. All the protocols for security route discovery used cryptographic methods to perform the security with establishment of associative security. To secure data communications, secure routing discovery is applied first to ensure the validity of the used routing path. For the data communication security, redundancy requires to obtain availability requirement.

In this paper [7], TRSDMP routing protocol is proposed which chooses the most spatially disjointed paths that could join to a partially trusted level via nodes that specify a certain security threshold. It exploits a trusted node to participate in the selected set of routes between a source and destination.

In this paper [8], it was presented a novel security enhancement scheme, namely, Secure Protocol for Reliable Data Delivery (SPREAD). The goal is to distribute the secret, first by secret sharing algorithm at the source node to generate message shares and then by multipath routing to deliver message shares across the network, so that in the event that a small number of shares are compromised, the secret message as a whole will not be compromised.

In this paper [9], multipath optimized link state routing (MP-OLSR) protocol is proposed. The extension of the single- path version includes a major modification of the Dijkstra algorithm, auxiliary functions, i.e. route recovery and loop detection to guarantee quality of service and a possible backward compatibility based on IP-source routing. It is stated that MP-OLSR can effectively improve the performance of the network and also be compatible with OLSR.

In this paper [10], it is mainly concerned with authentication and confidentiality during data transmission among the nodes in MANET. A novel approach is proposed for providing the authentication and enhances the data confidentiality. The signature scheme in the transmission designed by using polynomial symmetrical decomposition problem based on non-commutative division technique.

In this paper [11], an enhancement to a recently introduced routing strategy is proposed towards message security in MANETs, called as Enhanced Trust-Based Multipath DSR. First, a comprehensive discussion on prominent works on security in MANETs has been presented, along with their respective advantages and limitations. Second, it is discussed that proposed enhanced message security scheme (ETB-MDSR) and contrast it against our so-called benchmark scheme (TB-MDSR) in terms of design components and features, mainly the trust model components and the trust strategy for route set selection.

In this paper [12], a secure multipath routing is proposed for improving data confidentiality in MANET. Initially multiple paths are established between source and destination for data transmission. In the established paths, the monitoring nodes are chosen based on the parameters such as available bandwidth and residual energy using swarm intelligence. These monitoring nodes involve in malicious node detection and informing the source of the attack. When the source wants to transmit the data to the destination, it eliminates the path with malicious nodes and bypasses the data through other alternate path. Then a secure key management technique is deployed to defend against the malicious attack.

In this paper [13], a secure framework is depicted for multipath routing in wireless multi-hop network, which can be seen as a solution for end-to-end secure routing for wireless multi-hop ad hoc networks. This framework provides security against not only ad hoc routing but also data forwarding.

In this paper [14], it is proposed an adaptive topology control protocol for mobile nodes. The protocol allows each node to decide whether to support energy-efficient routing or conserve its own energy. Moreover, it can drastically shrink the broadcasting power of beacon messages for mobile nodes. It is proved that any reconstruction and change of broadcasting radius converge in four and five beacon intervals, respectively.

In this paper [15], an estimated distance (EstD)-based routing protocol (EDRP) is proposed to steer a route discovery in the general direction of a destination, which can restrict the propagation range of route request (RREQ) and reduce the routing overhead. In the EDRP, the change regularity of the received signal strength (RSS) is exploited to estimate the geometrical distance between a pair of nodes, which is called the estimated geometrical distance (EGD).

In this paper [16], an adopted topology control technique is proposed based on a localized algorithm, can maintain local connectivity which results in keeping global network connectivity although the network is dynamic. In the proposed topology update mechanism, the update interval in each node is determined based on the transmission range and mobility information of its adjacent nodes so that the network connectivity is guaranteed.

In this paper [17], it is compared several topology algorithms like centralised and distributed topology control algorithms. They also provided a comparison of these algorithms and suggest which algorithms may perform best. They also gave comment on the partitioning, routing, scheduling and latency issues that may arise due to topology adaptations in a mobile ad-hoc network.

In this paper [18], it is proposed a dynamic method is proposed to effectively employ k-edge connected topology control algorithms in MANETs. The proposed method automatically determines the appropriate value of k for each local graph based on local information while ensuring the required connectivity ratio of the whole network. The results show that the dynamic method can enhance the practicality and scalability of existing k-edge connected topology control algorithms while guaranteeing the network connectivity.

The paper is organized as follows. The Section 1 describes introduction about MANET, security goals and threats, topology control issue in MANET. Section 2 deals with the previous work which is related to secure topology control. Section

3 is devoted for the implementation of Efficient Secure Topology Control. Section 4 describes the performance analysis and the last section concludes the work.

3. IMPLEMENTATION OF EFFICIENT SECURE TOPOLOGY CONTROL PROTOCOL

In the proposed secure topology control, there are four phases involved. In first phase, we propose the efficient topology control approach which consists of minimal weight estimation and exchanging information, topology estimation.

In second phase, Cluster is formed and cluster head is chosen. In third phase, multipath is deployed to improve reliability. In fourth phase, messages are encrypted and decrypted using RS codeword.

3.1 Efficient topology control approach

In this section, the aim is to build energy-efficient topology for wireless multi-hop networks. It is modeled the topology of a wireless network with each node using its maximal transmission power as an undirected graph G = (L,R) in the two dimensional plane, where L = {l_1, l_2, ..., l_n} is the set of nodes in the network and E is the set of bidirectional links. The network may be heterogeneous, and hence each node L_i may have its own transmission power p_t which can be adjusted by itself. Assume that bidirectional links are concerned. Therefore the bidirectional link (l_i, l_j), R implies that both L_i and L_j are covered by each other. We define the physical neighbor set of each node L_i as

$$NT_s^t = \{l_k \mid (l_i, l_k) \in R(G)\} \qquad (1)$$

Each bidirectional link is assigned a weight which can be derived from the weight function w. Thus the weight of a link (l_i, l_j) can be expressed by w(i, j).

We use link weight to represent the energy consumption required in the transmission along a link and use path weight to represent the sum of all link weights of a path. Therefore, we define the minimal energy path as the path with the minimal path weight

The computation of w(i, j) usually relates only to l_i and l_j , at most to their neighbors. This makes it possible that each node runs according to the locally collected information. However, the algorithm will not miss any logical neighbor which is placed on some minimal energy path in the original network.

3.2 Cluster formation

In cluster creation, it is classified all the mobile nodes in the network into cluster head node and cluster member node. Cluster Head (CH) is one hop away from the other cluster member. In each cluster head, all the cluster members record its IP address and store it in to routing table. Even cluster head also records all the IP address of Cluster member in its routing table. In a cluster region, Cluster head keeps a neighbor table that records all the IP address of its neighbor cluster head.

Cluster member nodes exchange routing and data information through Hello Messages. A cluster member node includes its IP address into its Hello message and a cluster head adds the IP address of its cluster member into its Hello message as well.

In order to facilitate the cluster head route discovery process, cluster member keep the IP addresses of other cluster head that can hear. When the previous cluster head moves away or a cluster member does not receive five Hello packets continuously from its cluster head, it considers that the wireless link between cluster regions is broken. Thus, a cluster member chooses the latest refresh cluster head in its routing table as its new cluster head, which is one hop from it, or becomes itself a cluster head if it cannot hear any existing cluster head. After broadcasting its Hello right next packet, the selected cluster head is informed that a new cluster member has joined its group. The cluster member will obtain the confirmation of its new cluster head when it receives the Hello packet that carries its IP address.

3.3 Multipath Routing

In Multipath routing approach, multi-hop transmission can be implemented using two-hop transmission. When two-hop transmission is used, two time slots are consumed. In the first slot, messages are transmitted from the source to the relay i.e. buffer, and the messages will be forwarded to the destination in the second slot. The required capacity of this two-hop transmission can be derived considering the destined of each hop transmission. The transmission of each path hop has its own interference, which happens in different slots. Since the transmissions of the two hops cannot occur simultaneously but in two separate time slots, the end-to-end interference set of the multi-hop link is determined by the maximum of the two interference sets.

The reason for choosing multipath routing is that to improve the reliability of data transmission by sending duplicated data via multiple paths. If a packet is delivered to the destination, even if some paths fail. In the presence of multipath routing, higher energy consumption and the high probability of network congestion will happen. To overcome this issue, redundancy is applied using erasure coding on multipath routing. The idea is to send more fragments, P + N, than the minimum required fragments, P, to recover the original packet at the destination. In the proposed secure routing scheme, the reliability of packet transmission, the successful end-to end data delivery, is achieved by sending the fragments of RS codeword on *mq* selected node-disjoint multipath and to guarantee that the codeword packet is recoverable from any [*mq*/2] paths, it is required to ensure that fragments allocation on any [*mq* /2] paths follows,

$$\sum_{j=1}^{[mq/2]} y_j \geq N \qquad (2)$$

The wireless links of multipath are also authenticated indirectly, due to the cluster neighborhood authentication phase of the protocol. Since each node *mj* periodically authenticates its cluster neighborhood, each node may verify the authenticity of its own links as well as paths inside any routing path that it participates during the transmission.

In Route Request Query Transmission phase, each mobile node *mj* accepts a request query, only if the last mobile node identified in the partial *RouteQueryList* of the received route query message. It should be an authenticated neighbor of node *mj*. Moreover, during the route reply propagation, each node *mj* accepts and forwards a reply message, only if the two mobile nodes identified before and after Route_ID_j in the routing path $ni = (ID_S$, *RouteQueryLis*$_j$, ID_T) of the reply message, are authenticated cluster member neighbors of *mj*. Each node m_j only verifies if the node identifiers in concern belong to its current neighborhood Nt_i . The use of the authenticated cluster neighborhood is very efficient, since the cryptographic actions are performed once during a time period, regardless of the number of route request queries and route replies that pass through an intermediate node.

The duration of one time period is a system parameter that depends on how often the links as well as paths between mobile nodes are expected to break or to be established. It is decided that the indirect link authentication allows to a malicious node that is a neighbor of node to impersonate any other node. If indirect authentication is performed, impersonation may likely to occur, that the malicious node will not manage to exclude the original node *ni* from the routing paths, since the protocol allows to node *mj* to process all different incoming threads of a request query coming from the same node. So the impact of impersonation is useless.

3.4 Secure Encryption and Decryption phase

In this phase, both encryption and decryption schemes are implemented. Here three types of iterations are used while converting plaintext to ciphertext. In first iteration, plaintext is converted into ASCII value. In second, ASCII is converted into BCD value. In third, BCD is converted in to Hexadecimal value.

Step 1: Split the original data message of size W into *l* packets each of K fragments of size *d* bits. It is assumed that number of packets is equivalent to the number of paths used to transmit the data, *mq*, such that $Kd = \lceil W/mq \rceil$. If the last packet is less than K fragments, zero padding is applied to meet the length requirements of RS codes. It is nothing but adding zeros after the bit sequence.

Step 2: Perform the encoding operation on each packet using RS codes to generate K data fragments and M parity fragments as a codeword of size *M+K* fragments such that M ≤ K. For each codeword packet, allocate one fragment on each path starting from the highest secure path and repeat this process till all the *M+K* fragments are assigned on the selected multipath and ensure that the number of allocated fragments on each path, y_j, follows,

$$y_j = \left\lceil \frac{K+M}{mq} \right\rceil < K\, , j = 1,2,\ldots\ldots m \qquad (3)$$

Step 3: Based on the required security status, the number of fragments to be encrypted, M_{enc}, is calculated as follows:

$$M_{enc} = M + U \qquad (4)$$

Where *M* is determined according to the required security status and $1 \leq E \leq M$.

Condition 1:

For a low security requirement, U = 1, source node only encrypts any M_{enc} = *M* + 1 of *M* + *K* fragments from the codeword. For each codeword, an attacker must receive at least K of the *M* + *K* fragments and be able to decrypt the encrypted fragments to restore the codeword.

Condition 2: For a high security Requirement, then *U* = *M*, which requires to encrypt M_{enc} = *M+U* fragments for each codeword. In order to negotiate the data packet, the attacker must receive and be able to decrypt all *K* fragments to reconstruct the codeword.

Step 4: Forward all the fragments on the *mq* node-disjoint paths to the sink with each path carrying y_j

fragments. For enhancing the security, the encrypted fragments from the same codeword are transmitted on different paths.

Step 5: At the destination part, the encrypted data fragments are decrypted first and then all the fragments are decoded to recreate the original data packet.

3.5 Proposed Packet Format

Source and Destination	Next hop	Node Authentication	Hop count	IR	CRC
4	1	2	1	2	2

Fig.1.Proposed Packet format

In fig1, IR describes Interference ratio of each link. Cyclic Redundancy Check (CRC) for error correction and detection. Each physical neighbor (the destination) has an entry in the table. The node authentication represents the number of nodes is authenticated and identified the malicious nodes. The network topology under ESTCP is all the nodes in L and their individually perceived logical neighbor relations.

4. PERFORMANCE ANALYSIS

We use NS2 to simulate our proposed algorithm. In our simulation, 200 mobile nodes move in a 1000 meter x 1000 meter square region for 80 seconds simulation time. All nodes have the same transmission range of 300 meters. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 1.

Network Simulator (NS) is an event driven network simulator developed at UC Berkeley that simulates variety of IP networks. It implements network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations.Currently, NS (version 2) written in C++ and OTcl (Tcl script language with Object-oriented extensions developed at MIT) is available.

4.1 Performance Metrics

We evaluate mainly the performance according to the following metrics.

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

Packet Delivery Ratio: The packet delivery ratio (PDR) of a network is defined as the ratio of total number of data packets actually received and total number of data packets transmitted by senders.

Node degree: It is the important metric to evaluate the performance of topology control algorithms. If the node degree is higher, it indicates that higher collision will be. So value of node degree should be kept small.

Network connectivity ratio: It determines the nodes are connected in the intermediate region. It should be kept small while varying the average speed.

End-to-End Delay: The End-to-End delay is defined as the difference between two time instances: one when packet is generated at the sender and the other, when packet is received by the receiving application.

Table I. Simulation Settings and Parameters

No. of Nodes	200
Area Size	1000 X 1000
Mac	802.11
Radio Range	300m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	AODV
Packet rate	6pkts/sec

The simulation results are presented in the next part. We compare our proposed algorithm ESTCP with EETCA [20], NCTC [19] and DM [18] in presence of topology control environment. Figure 2 shows the results of connectivity ratio for varying the mobility from 5 to 25. From the results, we can see that scheme ESTCP has slightly lower connectivity ratio than EETCA, NCTC and DM method because of light weight calculations.

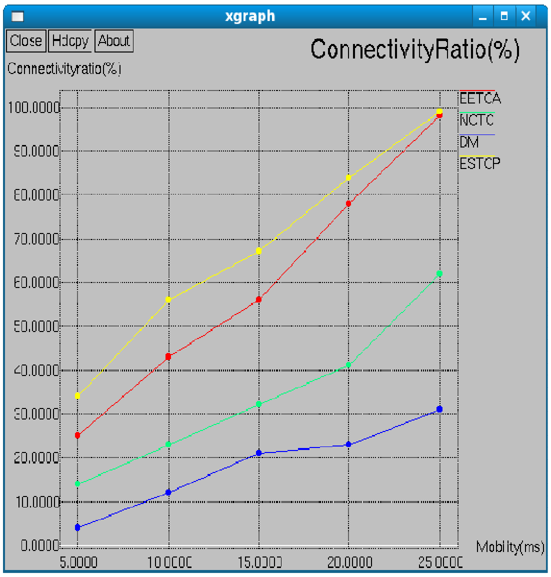

Fig.2. Mobility Vs Connectivity Ratio

Fig. 3, presents the comparison of node degree It is clearly shown that the node degree of ESTCP has low overhead than EETCA, NCTC and DM.

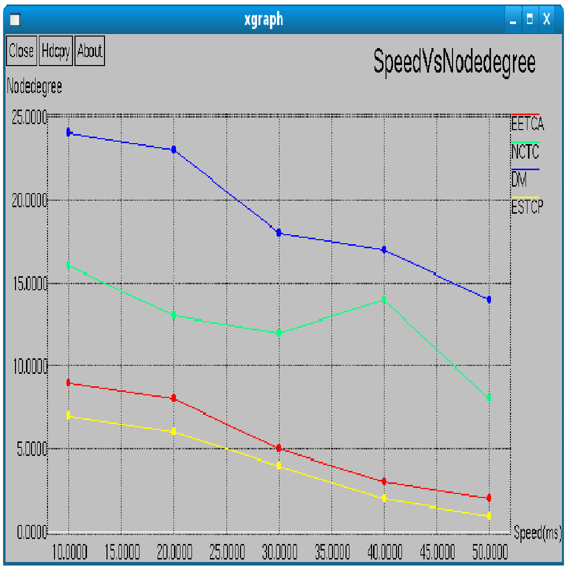

Fig. 3. Speed Vs Node degree

Figure 4 shows the results of Time Vs End to end delay. From the results, we can see that ESTCP scheme has slightly lower delay than EETCA, NCTC and DM schemes because of stable routes.

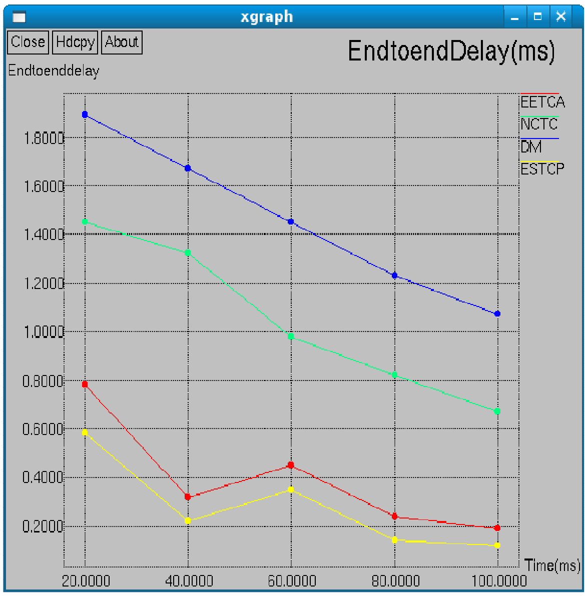

Fig. 4. Time Vs End to end delay

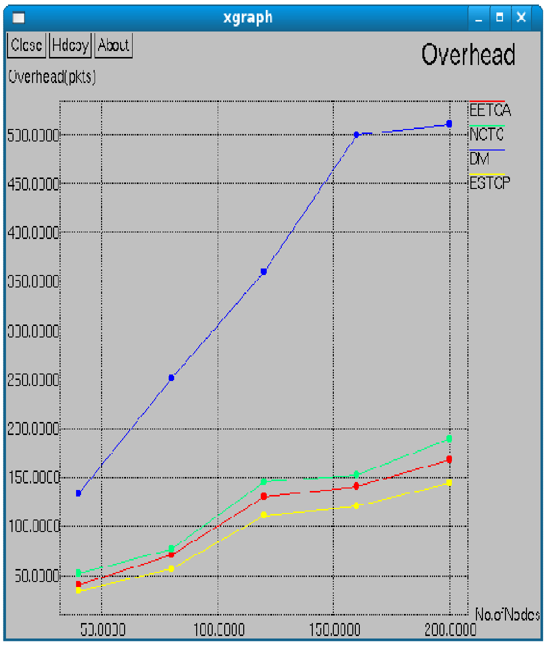

Fig.5.No. of Nodes Vs Overhead

Fig. 5, presents the comparison of overhead while varying the nodes from 0 to 200. It is clearly shown that ESTCP has low overhead than EETCA, NCTC and DM method.

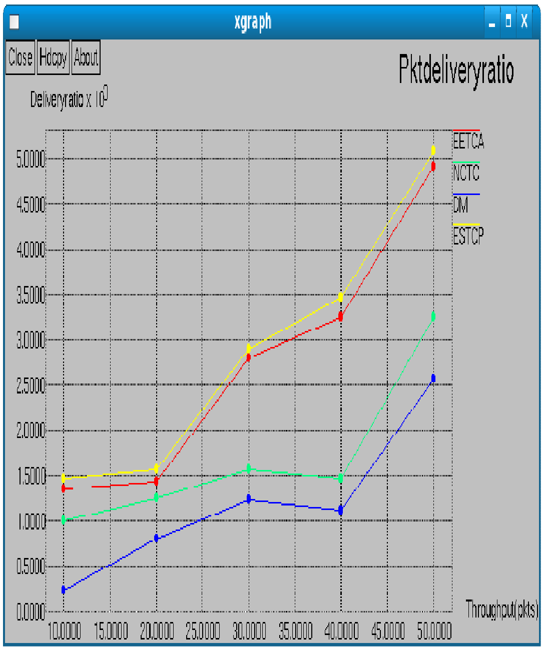

Fig.6. Throughput Vs Packet Delivery Ratio

Figure 6 show the results of average packet delivery ratio for the throughput 10, 20…50 for the 200 nodes scenario. Clearly our ESTCP scheme achieves more delivery ratio than EETCA, NCTC and DM schemes since it has both topology control features.

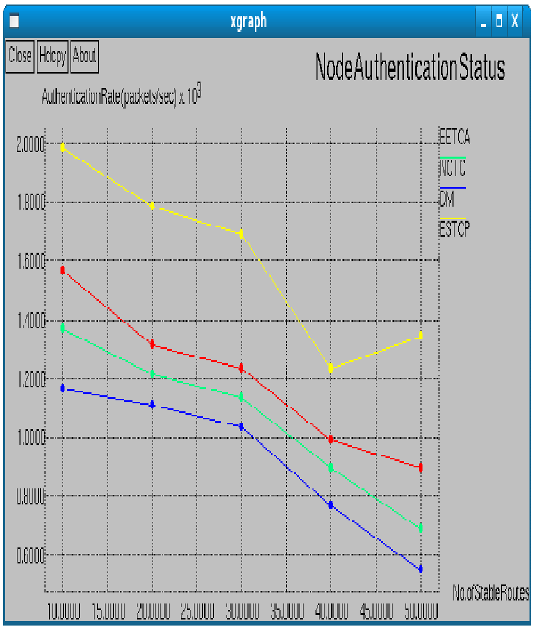

Fig.7.No. of Stable Routes Vs Node Authentication Rate

Figure 7 shows the results of Node Authentication Rate for varying the stable routes from 10, 20,…50. From the results, we can see that scheme ESTCP has slightly higher authenticate rate than EETCA, NCTC and DM method because of secure encryption and decryption scheme.

5. CONCLUSION

Mobile nodes are communicating without any access point in MANETs. Due to the uncontrolled topologies, the more interference and more energy consumption is introduced in the networks which leads to less performance of network connectivity. Moreover, the network performance will get degraded by means of attackers. In this paper, we have introduced the efficient secure topology control protocol to make the balance between the security and interference to improve the reliability. In first phase, efficient topology control scheme is introduced to extend the network lifetime of MANET. To improve the load balancing and network lifetime, multipath routing is used. Messages are securely transmitted and received using encryption/decryption scheme. By simulation results we have shown that the ESTCP achieves good packet delivery ratio, better network lifetime while attaining low delay, overhead, while varying the number of nodes, node velocity and mobility.

REFERENCES:

[1] Panagiotis Papadimitratos and Zygmunt J. Haas, “Secure Link State Routing for Mobile Ad Hoc Networks”, International Symposium on Applications and the Internet, 2003, pp.1-5.

[2] Rajneesh Narula, Sumeer Khullar, Kaushal and Anish Arora, “Security Issues of Routing Protocols in MANETs”, International Journal of Computers & Technology, Vol.3, No.2, 2012, pp.339-342.

[3] M .Nasir Iqbal, Junaid A.Khan, Farooq Umer, Nadeem Javaid, Izhar-ul-Haq and Mustafa Shakir, “Security Enhancement of Pro-active Protocols in Mobile Ad-hoc Networks”, Journal of Basic and Applied Scientific Research, Vol.3, No.3, 2013, pp.101-107.

[4] Danai Chasaki, Y. Sinan Hanay and Tilman Wolf, “Topology Reconstruction via Path Recording in Secure MANET”, IEEE conferences, 2008, pp.1-7.

[5] A.Prabhakaran and G.Vijayanand, “Secure Design for Topology Control And

Authentication in MANET", International Journal of Futuristic Science Engineering and Technology, Vol.1, Issue 2, 2013, pp.127-132.

[6] Salwa Aqeel Mahdi, 1Mohamed Othman, 1Hamidah Ibrahim, 2Jalil Md. Desa and Jumat Sulaiman, "Protocols For Secure Routing And Transmission in Mobile Ad Hoc Network: A Review", Journal of Computer Science, Vol.9, No.5, 2013, pp. 607-619

[7] Musab Ahmad AL-Tarawni and Dr. Mohd.Yusoff Jamaluddin, "Trusted Route of Spatial Disjoint Multipath Routing over MANET", International Journal of Applied Science and Technology, Vol. 3 No. 4; April 2013, pp.49-54.

[8] Wenjing Lou, Wei Liu, Yanchao Zhang and Yuguang Fang, "SPREAD: Improving network security by multipath routing in mobile ad hoc networks", Wireless Networks, Springer, Vol.15, 2009, pp.279-294.

[9] Jiazi Yi, Asmaa Adnane, Sylvain David, Benoît Parrein, "Multipath optimized link state routing for mobile ad hoc networks", Ad Hoc Networks, Elsevier, Vol.4, 2010, pp.1-20.

[10] G. S. G. N. Anjaneyulu*, V. Madhu Viswanatham** and B. Venkateswarlu, "Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks", Advances in Applied Science Research, Vol.2, No.4, 2011, pp.177-186.

[11] Lubaid Ahmed, "Trust-enhanced secure multipath routing for mobile ad hoc networks", Thesis and dissertations, Digital Commons, Ryerson University, pp.1-98.

[12] 1P. Sandhya and 2Julia Punitha Malar Dhas, "Secure Multipath Routing for Data Confidentiality in Mobile Ad Hoc Networks", Research Journal of Applied Sciences, Engineering and Technology, Vol.6, No.13, 2013, pp.2415-2422.

[13] Binod Vaidya, Dong-You Choi, JongAn Park and SeungJo Han, "Investigation of Secure Framework for Multipath MANET", International Journal of Security and Its Applications, Vol. 2, No. 4, 2008, pp.21-28.

[14] Andy An-Kai Jeng and Rong-Hong Jan, "Adaptive Topology Control for Mobile Ad Hoc Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 12, 2011, pp.1953-1960.

[15] Xin Ming Zhan, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, "An Estimated Distance-Based Routing Protocol for Mobile Ad hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 60, No. 7, 2011, pp.3473-3484.

[16] Atsushi Yoshinari, Hiroki Nishiyama, Nei Kato, and Dan Keun Sung, "Dynamic Topology Update Mechanism in Local Tree-based Reliable Topology (LTRT) based MANETs," IEEE International Conference on Communications (ICC 2012), Ottawa, Canada, Jun. 2012, pp.1-6.

[17] Gaurav Srivastava, Paul Boustead and Joe F.Chicharo, "A Comparison of Topology Control Algorithms for Ad-hoc Networks",

[18] Hiroki Nishiyama, Thuan Ngo, Nirwan Ansari, and Nei Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks," IEEE Transactions on Wireless Communications, vol.11, no.3, pp.1158-1166, Mar. 2012.

[19] T.S.Asha and N.J.Muniraj, " Network Connectivity based Topology Control for Mobile Ad Hoc Networks", International Journal of Computer Applications, Vol.56, No.2, 2012, pp.26-31.

[20] T.S.Asha and N.J.Muniraj, "Energy Efficient Topology Control Approach for Mobile Ad hoc Networks", International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, 2013, pp.289-296.