Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/110423

Detecting and Denying Malicious Behavior using Adaptive Learning based Routing Protocol in Wireless Mesh Network

R. Regan[1,*] *and J. Martin Leo Manickam*[2]

[1] Department of CSE, University College of Engineering, Villupuram, Anna University, India
[2] Department of ECE, St.Joseph's College of Engineering, Chennai, India

Received: 11 Apr. 2017, Revised: 24 May 2017, Accepted: 26 May 2017
Published online: 1 Jul. 2017

Abstract: Wireless Mesh Network (WMN) is a self organization and self configuration network which provides fast internets based on hybrid network. WMN consists of mesh nodes and mesh routers which provide security to sufficiently analyze the location but its performance is degraded when it comes to its overhead. WMN provides different security solutions at different levels of its layers. Each and every layer encounters attacks by the malicious behavior program which is due to the presence of its layers. So, in this paper, we propose a new framework solution against wormhole attacks based on adaptive learning technique, which provides mesh node level security and cluster head level security for avoiding wormhole attack. This framework focuses on routing layer which updates malicious node details and faster analysis of mesh routers. The performance has improved in terms of packet delivery ratio, routing overhead, throughput, and end to end delay compared to the Control Traffic tunneling Attacks Countermeasure (CTAC).

Keywords: Wireless Mesh Network, Wormhole attack, Data traffic tunneling, node separation, control traffic tunneling

1 Introduction

A Wireless Mesh Network (WMN) can be categorized into infrastructure WMN, Node WMN and Hybrid WMN [1], which are progressively self organized and self configured. Hybrid WMN has to coordinate different types of networks such as WiFi, sensor, WiMax, and IEEE802.16. It integrates the mesh node and mesh router by automatically building up and keeping up mesh networks themselves. WMN provides an assurance to run various applications in wireless technology. Mesh nodes can be desktops, PDAs, packet PCs, and phones . But, in mesh node correspondence conventional communication protocols is light-weight, and which does not exit the gateway and bridge technology [2]. So, just a communication interface is required in a mesh node. The mesh node also acts as a router for mesh networking. The equipment and programming are much easier to use mesh nodes. Hence, mesh nodes have consumed different applications that control and arrange the data streams to and from mesh nodes or mesh router. As indicated by the security Act of 2007, small network data communication provides secure exchange end-to-end, two way interchanges. Hence, Mesh router has provided minimal security and minimal movement, which creates an accessing structure for mesh node [3]. Next generation cellular network will yield high speed data rates to users with different geographical position, based on LTE technology and WIMAX. But, wireless mesh network coordinates existing network and gives feasible solution to users. [4] Wireless network security has major problems to physical channel data transmission, because, energy level of channel fluctuates due to mobility of nodes in mesh network. Thus, computational complexity is very challenging at routing layer of mesh router, with Security and privacy issues whose statuses are discussed in the background section and these cause issues on different situations and settings. Different network systems have been reviewed for security issues which provide different results based on their prevailing conditions. A framework setting compares design parameters for working the backhaul network, for example scheduling, transmission path energy, and traffic variations. The proposed method advantages, by Adaptive Learning based Routing Protocol (ALRP), it is possible to

* Corresponding author e-mail: reganr85@gmail.com

provide correct decisions required over time for the data transmission / reception among multiple networks. Through traffic control and data traffic management we can easily handle wormhole attack when it is created and identified in an efficient manner.

1.1 Aims and Objectives of adaptive learning based routing protocol

The aims and Objectives of adaptive learning based routing protocol; the main aim of this research work is to identify the routing layer security issues on hybrid network over WMN. To mitigate the mesh router routing challenges without the need to highlight the path of resistance. To provide an efficient framework to routing in future considering the requirements of mesh routing metrics such as delay, bandwidth, and resource allocation. During the data transmission, security issues plays a vital role in the wireless mesh network, since the security issues arise from different levels of layers of WMN. We mainly focus on routing layer of WMN [5]. If any malicious behavior program is running, then the WMN network bandwidth resource is prone to attacks. Different types of attacks may have their varying impacts on routing layer [6]. These are control traffic attacks, data traffic attacks, rushing, Sybil, grayhole, wormhole, routing table modification attacks, false routing control message attacks, routing buffer memory attacks, hop count manipulation attacks and reduced resource utility. We find it difficult to protect the network resources from attacks. hence, we propose a new framework to provide a feasible solution to this problem.

The rest of this paper is organized as follows: in section II background studies are summarized. Section III system model of adaptive learning based routing protocol and their limitations. The proposed method level one: two hop information of mesh node and level two: learning procedure of mesh router in section IV and V. Section VI shows the performance of adaptive learning based routing protocol and section 7 concludes the work.

2 Background Study

In the hybrid wireless mesh network, the malicious node can modify the normal activity of the network performance. The SDES [7] is a stream cipher-system for wireless network. It uses an authentication server which provides key in synchronism to access point. So, if synchronized type is followed, the intruder cannot access key. Stream cipher provides very simple encryption and decryption processes which consist of two shared keys. They are secret authentication key and secret session key both of which are used during the encryption process. This protocol is against key compromise, biased bytes analysis and integrity violation attacks. Two levels of security are used on adaptive learning based routing protocol in a hybrid network to create a standalone system. So, in this paper we propose two levels of security mechanisms. Threshold and identity-based key management [8] are further classified as authentication and key management schemes, in which each node is assigned an IP address during the life time of network services. Threshold and identity-based key management is of two phases. They are identity based authentication and distributed key generation. Both of them generate a master key in the first phase and public/private key generation in the second phase which offers high security based authentication mechanism. Exemplary, in this paper two types of keys are shared by mesh nodes which are private and public keys through KDC. Wireless intrusion detection and response system [9] is an intrusion detection system (IDS) for wireless network that works at low level of network layer. It tracks intruders based on MAC address filter and it does not collect MAC address of nodes in wireless network. It automatically detects suspicious node based on ARP poisoning. It is an efficient scheme of WMN, owing to secure authentication and access control mechanisms and performs two way authentication using mesh node and mesh router. Mesh node authenticates mesh router at transport layer security. Mesh node generates Center of Authentication (CA) with AAA [10]. When a mesh node is updated by a mesh router, mesh router interacts with a key distribution server for obtaining the key list which in turn shared among others. So, it does not intricate any issues such as message integrity, authentication and protection against reply attacks. It is an on-demand routing protocol that assumes clock synchronization and the existence of a shared secret between each pair of nodes. It also assumes an authentic TESLA [11] key for each node in the network and an authentic route discovery chain element for each node by which this node will forward RREQs. TESLA keys are distributed among the participating nodes via an online key distribution center. [12], Intermediate nodes are allowed to optionally reply to RREQs. It is resistant to replay, DoS, and routing table poisoning attacks. It is vulnerable to location disclosure, black hole, and wormhole attacks. [13], A trusted entity is also assumed which signs the public-key certificates for each node. Two types of leashes are distinguished- geographical leashes and temporal leashes. In case of geographical leashes, the scheme assumes geographical location information and loosely synchronized clocks. So, for faster verification purpose we use the adaptive learning based routing protocol with bloom filter in cluster head.

3 System Model of Adaptive Learning Based Routing Protocol

Mesh router utilizes two types of channels, one channel each is from mesh router to mesh node / mesh router.

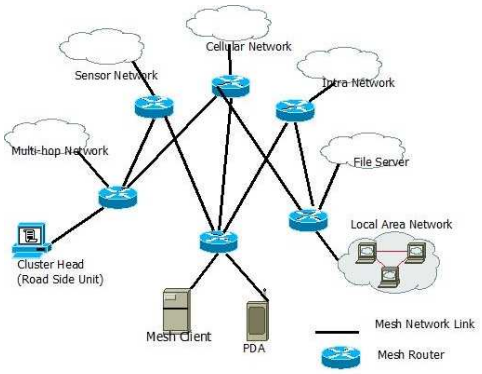

Fig. 1: Hybrid network of Wireless Mesh Networks

Each and every device of wireless mesh network uses an omni-directional antenna which shows in Fig 1. The contributions of the proposed approaches are represented.

–Two level security mechanisms are used(mesh node and mesh router)
–Level one : Two hop information of mesh node
–Level two : Learning procedure of mesh router
–Detecting and eliminating malicious nodes in the hybrid network through cluster head with mesh node.

3.1 Applications of ALRP:

Adaptive learning based Routing Protocol (ALRP) are quickly turning into the requirement of real world applications in society monitoring applications, military environment, battlefields, traffic management, security, and so on. This might be aided gathering neighboring node's details and additionally, they can give amazing information securing and choice making competencies. Also, ALRP gives better robustness, including reactions to sudden condition and in addition basic circumstances. In various situations and uses of MANETs, a node might dependably transform the speed and travel direction. So, it could create a problem on the organize topology. Therefore, the routing table of nodes is frequently updated nodes' details and also quickly updated in the neighboring nodes. Towards increasing the attackers, the system encounters more interruption and decrease in the benefit. So, analysis the computation complexity of MANET nodes [14]: Practically of the existing systems have high computational processing costs, due to the plan of their identification mechanism. The intrusion of detection systems can to the identification of affected node by attackers for limited nodes, but it doesn't apply larger node. This framework gives best results.

4 Level One: Two Hop Information of Mesh Node

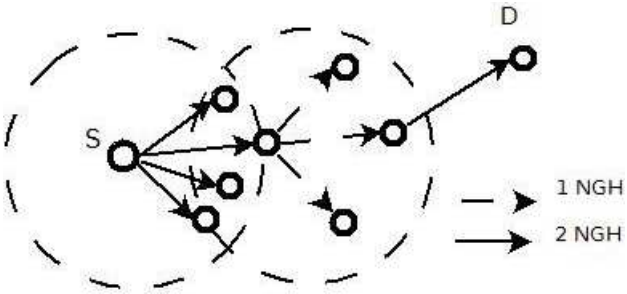

Fig. 2: Forwarding member S acts as a sender node to deliver an IP packet to node D

The situation for a forwarding set is shown in Fig 2. Here, the dark shaded coverage area represents the 1-hop NeiGHbor (NGH) forwarding space that relies on the destination direction. These three sets of node are unit accessible in Fig 2. A sender node demands communication with the destination. Furthermore, one-hop mesh node needs to communicate their cluster head when it does not embrace the marked mesh nodes to enhance the IP packet delivered to destination. Each mesh node may generate two types of keys which are public and private keys through Key Distribution Center (KDC) [15]. Public key is used to authenticate forward node and private key is used to authenticate destination when a packet has arrived at the mesh node.

Table 1: Notation with Description

Notation	Description
S, S_{IP}	Source node and its IP address
D, D_{IP}	Destination node and its IP address
FN, FN_{IP}	Forwarding node and its IP address
$S_{PATH\ LENGTH}$	Neighbor hop count list between source and destination
$D_{PATH\ LENGTH}$	Neighbor hop count list between destination and source
$K_{SESSION}$	Session Key
K_{AUTH1}	One-hop authentication key
K_{AUTH2}	Two-hop authentication key
$K_{PRIVATE\ AUTH}$	Destination node authentication key
SNM	Sequence number of message
H(.)	Hash function used by mesh node and mesh router
$MN_{(X,Y)}$	Current position details of mesh node like latitude, longitude
M	Message or payload
N_{MAC}	Medium Access Control address of participating node
RREQ	Route request message
RRESP	Route response message
//	Comment
H_COUNT	Hop count between source node and destination node
CH	Cluster Head of hybrid network

Two-hop handshake process has four possibilities. These are source to forwarding node, forwarding node to

another forwarding node, forwarding node to destination node, and source node to destination node.

```
Procedure: Two-hop handshake of mesh nodes
1. Whenever a source node S wants to communicate
   to a destination node D, S uses RREQ message
   packet and D uses RRESP message packet which
   propagates signals over the hybrid networks.
 1.1 SPATH_LENGTH = It collects each forwarding
     nodes path as a S to a D node when route
     RREQ packet is used. It will return number
     of hops with expected arrival time which
     is updated in routing table of FN and S.
 1.2 DPATH_LENGTH = It collects each forwarding
     nodes path as a D to a S node when route
     RRESP packet is used. It will return number
     of hops with expected with arrival time
     which is updated in routing table of FN and S.
 1.3 // S procedure for  triggering neighbor mesh
     node detection list
   1.3.1 For (i = 0; i < SPATH_LENGTH; i++)
   1.3.2 For (j = 0; j < DPATH_LENGTH; j++)
   1.3.3 if (min_path(S,D))
   1.3.4 // S generates authentication message
   1.3.5 S generates(FNIP, SNM, H_COUNT, M,
         KSESSION, KAUTH1, KAUTH2)
   1.3.6 // When S sends message to FN
     1.3.6.1 if(D is immediate neighbor of FN)
     1.3.6.2 S broadcasts(FNIP, SNM, H_COUNT,
             M, KSESSION, KAUTH1, 0)
     1.3.6.3 else
     1.3.6.4 // To apply Two-hop authentication
             key steps
   1.3.7 // When S sends message to D
     1.3.7.1 if (D is immediate neighbor of S)
     1.3.7.2 S broadcasts (DIP, SNM, H_COUNT, M,
             KSESSION, KPRIVATE _AUTH)
     1.3.7.3 // D applies hash function on
             received message
     1.3.7.4 if (D detects both authentication
             key and session key values are
             replica of those received from S)
     1.3.7.5 // to accept received message
     1.3.7.6 else
     1.3.7.7 // to deny received message
   1.3.8 // when message packet is forwarded from
         one-hop FNIP to two-hop FNIP
     1.3.8.1 if (message arrives at one-hop)
     1.3.8.2 S broadcasts (DIP, SNM, H_COUNT, M,
             KSESSION, KAUTH1, 0)
     1.3.8.3 if (message arrives at two-hop)
     1.3.8.4 FN broadcasts (DIP, SNM, H_COUNT, M,
             KSESSION, KAUTH1, KAUTH2)
     1.3.8.5 // to accept received message
   1.3.9 // when message packet is forwarded from
         FNIP to D
     1.3.9.1 if (message arrives at D)
     1.3.9.2 FN broadcasts (DIP, SNM, H_COUNT, M,
             KSESSION, KPRIVATE_AUTH)
```

5 Level Two: Learning Procedure of Mesh Router

The framework of adaptive learning based routing protocol has been allocated a small portion of memory to mesh router which applies security constraint using proposed method with Bloom filter technique as a randomized data structure which is represented as a stream set to store elements. However, hybrid network IP packets are analyzed using cluster header that takes input of IP Packet header information such as position, IP address, and MAC address to use membership queries on stream set of proposed method which may return false positive or false negative [16].

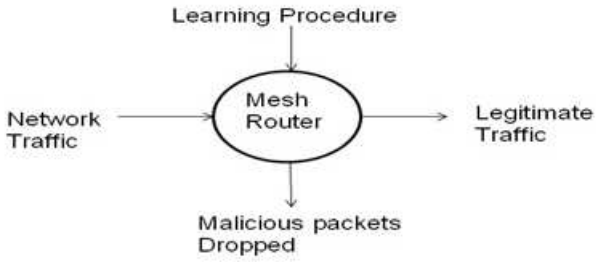

Fig. 3: Learning procedure of a mesh router in the WMN

Cluster header is used always to check IP packets if any one of the packets are forwarded over their network which is analyzed whether a packet is trusted or not, by utilizing the security framework and bloom filter technique.

Condition of false positive and false negative:

–Probability that a malicious node detail is not hashed after insertion of the node details f.

$$f = \left(1 - \frac{1}{m}\right)^{k} \tag{1}$$

–Py (Hashed value is not set to 1 after insertion of a malicious node details in n element)

$$Py = \left(1 - \frac{1}{m}\right)^{kn} \tag{2}$$

–Py (Hashed value is set to 1 after insertion of a malicious node details in n element)

$$Py = \left[1 - \left(1 - \frac{1}{m}\right)^{Kn}\right]^{k} \tag{3}$$

In the proposed method we use an array of n bits and k hash functions h1jhk , where k is a small constant value. Hash function helps us to store malicious node IP address and MAC address and their position details for future verification purpose in Fig 4.

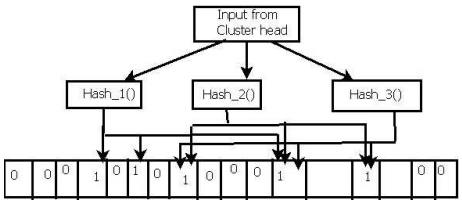

Fig. 4: Bloom Filter techniques works on cluster head

5.1 Steps to perform an adaptive learning based routing protocol

Step 1:The sender node attains the destination location using Global Positioning System (GPS) or location discovery algorithms.
Step 2:Forwarding node collects two hops information of mesh nodes within a cluster
Step 3:Cluster head is updated the position of mesh nodes through GPS/location discovery algorithms of their coverage area by updating each nodes own memory.
Step 4:Ensure IP address, MAC address and location details of the presence of packet.
Step 5:If the buddy list is non zero, it triggers first level security mechanism.
Step 6:If the forwarding list is zero, it triggers second level security mechanism.
Step 7:Later, the communication path is allocated to the forwarding node towards destination.
Step 8:Finally, to measure authentication delay, throughput, and energy level of mesh node and router and which full processing information.

Procedure: void FN of hybrid network to CH handshake

```
Whenever a FN is not communicating towards
destination node D.
  1.1 CH triggers path handling schemes
      while finding and avoiding malicious
      node.
  1.2 if (router is ensured of wormhole
      attack activated by malicious node
      by the FN)
  1.3 if (CH is ensured of FNIP and NMAC
      address of void FN that are newly
      updated in their CH and whether FN
      encounters congestion problem)
  1.4 // void handling scheme is activated
      incase if message packet has reached
      destination.
  1.5 else
  1.6 // CH triggers adaptive learning
      procedure using bloom filter technique
```

6 Performance Evaluation of the Proposed Adaptive Learning Based Routing Protocol (ALRP)

6.1 Simulation Setting

In this section, we have designed hybrid mesh network in network simulator- 2. The parameters obtained from proposed method are assigned for simulation entity with their limitations as shown in Table 2.

Table 2: Simulation input parameters

Parameter	**Values**
Simulation time	900 s
Channel bandwidth	2 Mbps
Transmission time	250 ms
Terrain area	1500 × 1500 m
Number of nodes	60-90-150
Traffic model	CBR
Mobility model	Random way point
Average Number of neighborhood nodes	5-9

The performance of adaptive learning based routing protocol is measured over unsecure hybrid network for the simulation purpose. Mesh nodes can be randomly (any to any) positioned. The message packets are exchanged among mesh nodes of 60, 90, and 150 within the 1500 × 1500 m area. The proposed adaptive learning based routing based protocol is compared with the existing CTAC [17]. The proposed method of implementation focuses on Quality of Service (QOS) when malicious node misbehaves on hybrid mesh network.

Table 3: Simulation results

No. of mesh nodes	Void forwarding node latitude	Void forwarding node longitude	No. of malicious nodes	No. of mesh routers deployed	Throughput (Mbps)	False positive ratio
10	6.623	67.480	2	1	1.793	0.003
20	8.342	62.732	4	1	1.923	0.007
30	3.452	73.823	6	1	1.453	0.009
40	2.863	42.767	8	2	1.307	0.012
50	3.672	32.627	10	2	1.109	0.015
60	8.411	82.327	12	3	1.003	0.019
70	4.456	55.672	14	4	1.459	0.025
80	2.862	73.822	16	4	1.763	0.027

6.2 Successive packet delivery ratio of message packet

The successive packet delivery ratio of the hybrid mesh network from source node S to destination node D node is shown in fig 5. It describes the number of message packets successfully delivered when malicious nodes are increased or the delivery ratio gets degraded. The proposed adaptive learning based routing protocol restricts the two-hop forwarding and void nodes.

Furthermore, the message packets are forwarded from S to D based on different levels of security. The prediction of cluster head, whenever malicious nodes activate wormhole attack on message packets in their network which will be denied is based on proposed method. It will provide correct guidelines to mesh nodes and to drop malicious packets until the malicious node is removed from their groups.

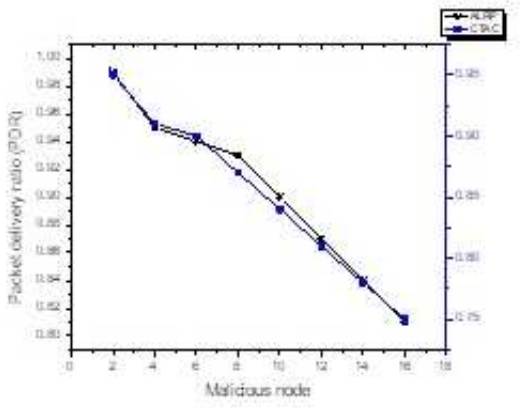

Fig. 5: Successive packet delivery ratios vs. malicious nodes

6.3 Overhead of cluster head when malicious nodes get increased

When hybrid network traffic increases certain parameters like RREQ, RRESP and Route error, the normal mesh node changes its behavior as a malicious node. So, cluster head always monitors their nodes whose results are shown in Fig 6. If the number of malicious nodes increases, the cluster head performance is reduced which has been compared with the proposed method of adaptive learning based routing protocol vs. CTAC.

6.4 Authentication delay on void forwarding node

When message packet is reaches a void node it is not forward to destination. So, it will obtain authentication processes from their cluster head. The elapsed time is called authentication delay. Cluster head provides the legitimate path information of trusted node. If any malicious node activates wormhole attack on receiving packets when it is being forwarded, then cluster head drops packets and that malicious node will attack nodes of this groups which will update all other mesh nodes. Fig 7 shows authentication delay of void forwarding node for adaptive learning based routing protocol vs. CTAC.

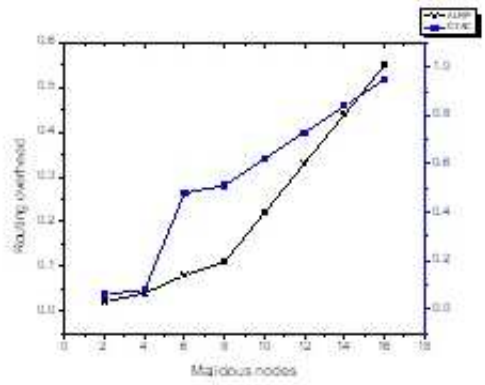

Fig. 6: Comparisons between the adaptive learning based routing protocol vs. CTAC

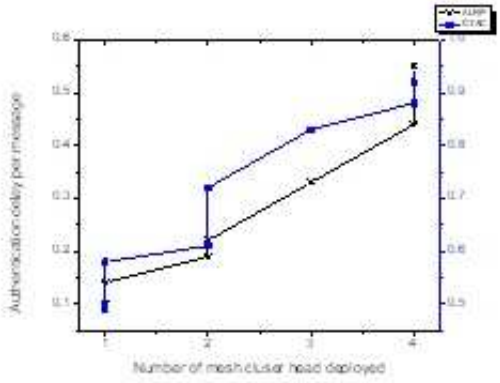

Fig. 7: Authentication delays per message vs. Number of mesh routers deployed in hybrid network

6.5 Cluster head to detect malicious activity before and after deploying adaptive learning based routing protocol

The participating mesh nodes and channel information are monitored by cluster head. The cluster head is used to detect malicious activity before and after deploying adaptive learning based routing protocol which is shown in Fig 8. Here malicious node increases the delay before usage of adaptive learning based routing protocol which is compared with the proposed method by applying two levels of security constraints on most of the non-misbehaving malicious nodes in hybrid mesh node due to their removal from their cluster.

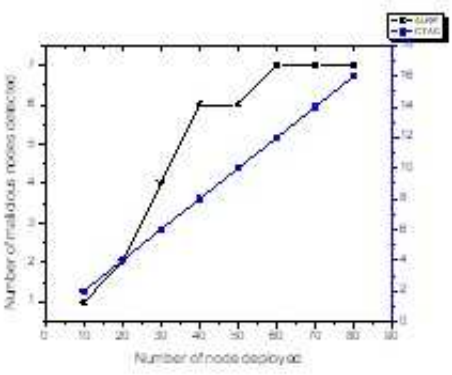

Fig. 8: Cluster head to detect malicious activity before and after deploying adaptive learning based routing protocol

6.6 Increased False positive rate vs. packet drop ratio increased

In the proposed method adaptive learning based routing protocol with bloom filter technique [18] has been used to in cluster header when forwarding node gets into void area, to suggest alternative path with proper grant from of cluster header. It is verified whether forwarding nodes IP address is either false positive rate or false negative rate. If The forwarding nodes IP is obtained as false positive rate, packet drop ratio increases which is shown in Fig 9.

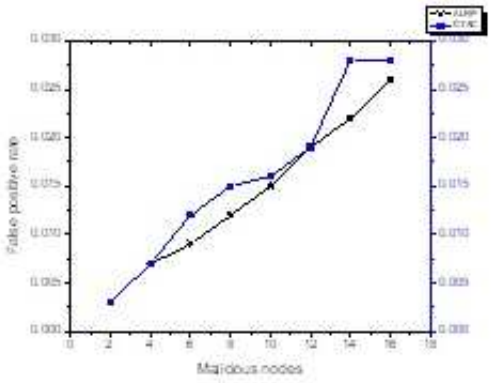

Fig. 9: False positive rates vs. Throughput

7 Conclusion

In this paper we have proposed an adaptive learning based routing protocol and it is compared with CTAC protocol. Both of them ensure reliable security but adaptive learning routing scheme prevents the network layer attacks in a hybrid mesh network. It is compared with CTAC to provide higher security, faster false positive rate and less authentication delay per message. A natural continuation of adaptive learning based routing protocol is stimulated and the result of simulations to verify variations in relevant factors or limit. From the show results from Fig-5 to Fig-9 ALRP tested and demonstrable itself and says it is an efficient method and its performance is better than the existing approach CTAC. ALRP can be applied video stream security using rational cryptography method.

References

[1] Admir Barolli, Tetsuya Oda, Makoto Ikeda, Leonard Barolli, Fatos Xhafa, Makoto Takizawa, ”Comparison Analysis by WMN-GA Simulation System for Different WMN Architectures, Normal and Uniform Distributions, DCF and EDCA Functions”, Advances on Broad-Band Wireless Computing, Communication and Applications, pp 129-142, 2016.

[2] Junhyung Kim, Jangkyu Yun, Mahnsuk Yoon, Keuchul Cho, Honggil Lee, Kijun Han, ”A routing metric based on available bandwidth in wireless mesh networks”, ICACT’10 Proceedings of the 12th international conference on Advanced communication technology Pages 844-849, 2010.

[3] A. A. Franklin and C. S. R. Murthy, An introduction to wireless mesh networks, book chapter in: Security in Wireless Mesh Networks, Y. Zhang et al. (eds.), CRC Press, USA, pp. 344. 2007.

[4] Sumit Kar and Srinivas Sethi, ”Security challenges in cognitive radio network and defending against Byzantine attack: a survey”, Int. J. Communication Networks and Distributed Systems, Vol. 17, No. 2, 2016.

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc05), Urbana-Champaign, IL, USA, pp. 46-47, May 2005, ACM Press.

[6] Nikam, P.D. and Raut, V. , Enhancement to EAACK for Improved MANET Security. International Journal of Advanced Research in Computer Science and Management Studies, 3, 324-329, 2015.

[7] H. S. Soliman and M. Omari, Application of synchronous dynamic encryption system in mobile wireless domains, in Proceedings of the 1 st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet05), Montreal, Quebec, Canada, pp. 24-30, 2005, ACM Press.

[8] H. Deng, A. Mukherjee, and D. P. Agrawal, Threshold and identity-based key management and authentication for wireless ad hoc networks, in Proceedings of International Conference on Information Technology: Coding and Computing (ITCC04), vol 1, pp. 107-11, April 2004. IEEE Computer Society Press.

[9] Y.-X. Lim, T. S. Yer, J. Levine, and H.L. Owen, Wireless intrusion detection and response, in Proceedings of Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, West Point, NY, USA, pp. 68-75, June 2003.
[10] N. R. Prasad, M. Alam, and M. Ruggieri, "Light-weight AAA infrastructure for mobility support across heterogeneous networks, Wireless Personal Communications, vol 29, no 3-4, pp. 205219, 2004.
[11] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, Efficient and secure source authentication for multicast, in Proceedings of the Network and Distributed System Security Symposium (NDSS01), San Diego, CL, USA, pp. 35-46, February 2001.
[12] D. B. Johnson, The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4, IETF RFC 4728, 2007.
[13] Y.-C. Hu, A. Perrig, and D. B. Johnson, Packet leashes: a defense against wormhole attacks in wireless ad hoc networks, in Proceedings of the 22nd IEEE Joint Conference of IEEE Computer and Communications Societies (INFOCOM03), San Francisco, USA, pp. 1976-1986, March-April 2003, IEEE Press.
[14] Erfan A. Shams1 Ahmet Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks", Wireless Network, 2017.
[15] Sumimol, L. and Janisha, A. Security in Wireless Adhoc Networks Based on Trust and Encryption. International Journal of Advanced Research in Computer and Communication Engineering, 4, 442-445, 2015.
[16] Sunil Kumar* and Kamlesh Dutta, "Intrusion detection in mobile adhoc networks: techniques, systems, and future challenges", Security Comm. Networks, 2016.
[17] Issa khail, M.Awad, CTAC: Control Traffic Tunneling attacks counter measures in mobile wireless network, Compueter networks, Sep 2012.
[18] Leonardo Maccari, Romano Fantacci, P.Neira, and R.M. Gasca Mesh network firewalling with bloom filters, cfsIEEE Communications Society subject matter experts for publication in the ICC 2007 proceedings, pp: 1546-1551, 2007.

R. Regan is working as an Assistant Professor in the department of Computer Science and Engineering at University College of Engineering Villupuram, Anna University, India. He acquired B.E. Degree in Electronics and Communication Engineering from Mailam Engineering College, Mailam in 2006. He received M.Tech. Degree in Computer Science and Engineering from Bharath University, Chennai in 2010. He is pursuing Ph.D. Degree in the Faculty of Information and Communication Engineering at Anna University, Chennai. He has over 5 years of experience in educational institution. He has to his credit 10 publications in National/International conferences and journals. His areas of interest include Mobile Ad hoc Networks, Wireless Sensor Networks, Wireless security.

J. Martin Leo Manickam is working as Professor in the Department Electronics and Communication Engineering at St. Joseph's College of Engineering, Chennai. He acquired B.E. Degree in Electronics and Communication Engineering from Alagappa Chettiar College of Engineering and Technology, Karaikkudi in 1995. He received M.E. Degree in Optical Communication and Ph.D degree in the Faculty of Information and communication Engineering from the College of Engineering, Anna University, Chennai. He has over 16 years of experience in teaching and guiding projects for Undergraduate and post graduate students. Under his guidance, One scholar had got Ph.D. degree and 12 research scholars are pursuing their Ph.D. programme. He has to his credit 15 publications in National/International conferences and journals. His areas of interest include Mobile Ad hoc Networks, Wireless Sensor Networks, Digital Communication and Network Security.