International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319 – 6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 4; April 2017; Page No. 3555-3558
DOI: http://dx.doi.org/10.24327/ijcar.2017.3558.0313

Research Article

A NOVEL AUTHENTICATED and STORAGE CONSTRAINED QoS ROUTING PROTOCOL USING ONION ROUTING IN MANETS

Sivapriya S[1*] and Naresh Kumar Thapa K[2]

[1]ECE Department, College of Engineering, Guindy, Chennai-20
[2]ECE Department, Velammal Engineering College, Chennai-68.

A R T I C L E I N F O

Article History:

Received 25th January, 2017
Received in revised form 19th February, 2017
Accepted 22nd March, 2017
Published online 28th April, 2017

Key words:

Mobile ad-hoc network (MANET), QoS Aware Routing protocol, ONION encryption, TOR (The Onion Router).

A B S T R A C T

Researchers in the field of ad-hoc wireless communication network have targeted mostly on the design of security aspects such as confidentiality, integrity, authenticity and reliability in Mobile ad hoc network (MANET). Securing data dissemination between these nodes in such networks, however, is a very challenging task. Exposing such information to anyone else other than the intended nodes could cause a privacy and confidentiality breach, particularly in military scenarios. In this paper, we proposed a novel framework which increases the security and privacy over MANETs. We used TOR networks with storage constrained QoS aware routing makes anonymity for its client by routing the client packets via various volunteering networks, such routing conceals the client's location & activity thus making traffic analysis or network surveillances impossible by the intruders.

INTRODUCTION

Mobile ad hoc networks (MANETs) are vulnerable to security threats due to the open wireless medium and dynamic topology. It is difficult to provide trusted and secure communications in adverse environments. On one hand, the adversaries outside a network may infer the information about the communicating nodes or traffic flows by passive traffic observation, even if the communications are encrypted. On the other hand, the nodes inside the network cannot be always trusted, since a valid node may be captured by enemies and becomes malicious. As a result, anonymous communications are important for MANETs in adversarial environments.

The key to implementing the anonymous communications is to develop appropriate secure routing protocols. The actual route discovery starts with broadcasting RREQ (route request) packet to its neighboring nodes. The beacon frames is transmitted in a regular interval to check the nodes availability as mentioned in [3] and [4]. The routes have been selected based on storage constrained QoS aware routing protocol. The data is encrypted in form of layers, for each hop a layer is decrypted / removed & data is forwarded, so on at the end the last layer is decrypted & forwarded to destination. During the forwarding or hopping the actual content is invisible to the relay/mix nodes, thus the name onion routing.

Corresponding author:* **Sivapriya S
ECE Department, College of Engineering, Guindy, Chennai-20

Node to node communication is secured by public keys are used by communicating clients for establishing AES session keys for each hop. Hence in order to provide reliable communication, a MANET thus requires a reliable data delivery method that can adapt to a changeable network topology and an unstable wireless network.

QoS Aware Routing Protocols

QoS is a commitment that assures some guaranteed services such as bandwidth, delay, jitter, packet delivery ratio etc., As mentioned in [1], the basic quality of service parameters are packet delivery ratio, end-to-end delay and throughput which varies with different routing protocols methods. In this proposal, QoS based routing has been proposed that provides feedback about the available storage capacity throughout the route, so that data transmission takes place according to available storage capacity which satisfies requirement of the application.

Onion Routing

In the proposed system, our main aim is to increase the packet delivery ratio and decrease the average end-to-end delay. We have adopted storage capacity constrained QoS Aware Routing protocol for selecting the best route with storage capacity of intermediate nodes as cost metric and used ONION routing to improve security levels. Let us consider a group of nodes which are mobile which also includes malicious nodes. The source node initiates the route discovery process by sending RREQ to neighboring nodes. At the same time, the source node broadcasts beacon frames (HELLO

packets) to all intermediate nodes for identifying minimum hop count, capacity of intermediate nodes, based on node connectivity. The route selection is based on the constraint that the storage capacity of intermediate nodes should be greater than source node. On receiving RREQ, the destination responds back to source using RREP. Each intermediate node validates the RREP packet and updates its routing tables. After route selection, source encrypts the data based on AES encryption and it collects the selected neighbor nodes public key from routing table based on storage constrained QoS aware routing. Now the data establishment commences as source node forwards the encrypted packet to neighbor node based on selected route. Neighbor node gives its own private key for one part of decryption process. The process continues till it reaches the destination. Then the destination node decrypts the packet with its private key and AES decryption key. Finally destination node views the original data. In case if an intruder tries to open up the datagram with its private key, it is impossible as it is not wrapped up with its public key. Hence this is less prone to data hacking and increases packet delivery ratio (PDR). Since the paths capacity will vary dynamically, so that the paths will be changed dynamically as per data transfer along the network.

Protocol Architecture

The literature survey presented in references [6] & [7] used only onion encryption in application layer and no efforts are taken with regard to QoS parameters. The proposed systems have developed ONION & AES encryption in application layer and routing is based on capacity constrained routing in network layer.

The figure 1 represents protocol architecture layer which describes the process that takes place in different OSI layers in our proposed system.

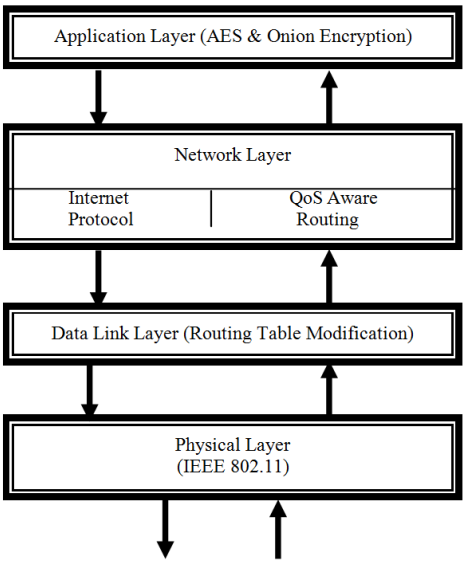

Fig 1 Protocol architecture layer of proposed system

Route Selection based on bandwidth constrained QoS protocol

Let us consider a group of nodes where each node has their own source-id, public key and private key.

Let us consider A as the source node and G as the destination node. Now the source node broadcasts the HELLO message request to its neighbouring nodes namely B, C and D. The HELLO message would be broadcasted to all its neighbouring nodes only within its transmission range.

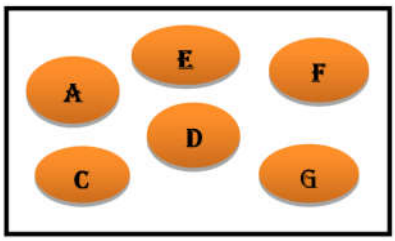

Fig 2 Formation of nodes in an area

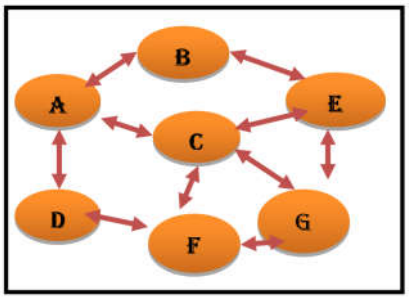

Fig 3 Broadcasting HELLO message request

The HELLO message requests from the source have reached the destination through multiple intermediate hops. All the intermediate nodes update their routing table with maximum capacity of all their neighbouring nodes. The destination node now calculates their route to the source based on how much capacity each node can handle which would exist more than the size of the data packet (transmitted along with the HELLO message request packet).

Let us consider the maximum storage capacity of a packet that a source node can transmit is 100Mb. Each intermediate node has a capacity of:

- Node B-200Mb
- Node C-50 Mb
- Node D-150Mb
- Node E-175Mb
- Node F-75Mb

Now the best route is selected which exceeds 100Mb (the maximum storage capacity of source node).The route from source to destination is A-B-D-E-G.

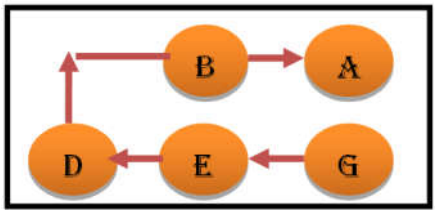

Fig 4 Sending RREP to the source node

Finally, the destination sends the RREP back to the source through selected intermediate hops.

Data authentication and Encryption

In the existing system [3] & [4], the data packets are single encrypted with different cryptographic techniques such as AES algorithm. We have proposed a novel authenticated routing protocol with multiple encryptions of data.

Finally the data which is multiple encrypted (AES + PRIMARY KEYS OF NEIGHBOURING NODES) is transmitted through the wireless channel. Now, the size of the data packet still gets reduced due to ONION encryption which eliminates packet dropping. The data which reaches the node B uses its private key and decrypt the message. The same process is repeated until it reaches the destination. At the destination, the node G uses its private key to view the original data.

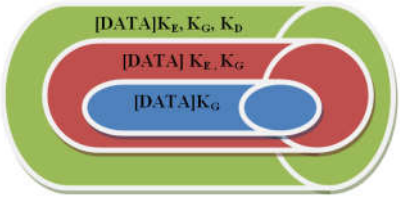

Fig 5 Data Encryption using onion routing

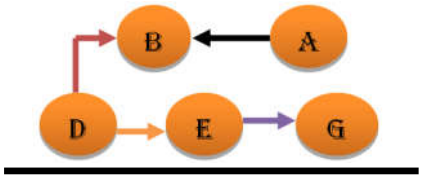

Fig 6 Data transmission using onion routing.

- [DATA] decrypted with private key of B
- [DATA] decrypted with private key of D
- [DATA] decrypted with private key of E
- [DATA] decrypted with private key of G

In case of any intrusion, the data can't be seen as far as the private key of the neighboring node is known. There won't be any packet dropping as it involves multiple layers of encryption and decryption with the assumption that every node are available with sufficient amount of power. Finally the data would reach the destination with less delay and high packet delivery ratio.

Mathematical analysis

Packet delivery ratio

Packet delivery ratio is one of the important factor to measure the performance of routing protocol in any network. The performance of the protocol depends on various parameters chosen for the simulation. The major parameters are packet size, no of nodes, transmission range and the structure of the network.

Packet delivery ratio is the ratio of number of packets received at the destination to the number of packets sent from the source. The performance is better when packet delivery ratio is high.

Mathematically it can be shown as equation (i):

$$PDR = Prx / Ptx \quad \text{---------- (i)}$$

where Prx is the packets successfully received and Ptx is the total number of packets created.

The above expression says the fact that PDR completely depends on the number of packets received and total number of packets transmitted. There is a increase in PDR from all other pre-existing protocols due to the selection of route which was based on the storage capacity of each mobile nodes.

Average End-to-End Delay

Average End-to-end delay is the time taken by a packet to route through the network from a source to its destination. The average end-to-end delay can be obtained computing the mean of end-to-end delay of all successfully delivered messages. Therefore, end–to-end delay partially depends on the packet delivery ratio. As the distance between source and destination increases, the probability of packet drop increases. The average end-to-end delay includes all possible delays in the network i.e. buffering route discovery latency, retransmission delays at the MAC, and propagation and transmission delay.

Mathematically it can be shown as equation (ii):

$$D = (1/n) \sum_{i=1}^{n} (Tri - Tsi) \quad \text{---------- (ii)}$$

where, D = Average End to End Delay
i = packet identifier
Tri = Reception time
Tsi = Send time
n = Number of packets successfully delivered

From the above expression, the average end-to-end delay is considerably reduced due to onion encryption which in turn leads to less packet loss.

SIMULATION RESULTS AND DISCUSSIONS

The simulation have been performed under NAM (Network Animator) and NS2 (Network Simulator 2) environment. The simulation parameters have been listed below in table1.

Table 1 Simulation Parameters

Parameters	Values
Source Type	MAC IEEE 802.11
Packet Sixe	512 BYTES
Terrain Size	1500*1500
Traffic Size	CBR(constant bit rate)
Number of Nodes	100
Transmission Range	250m

The following are the inferences made from the simulations:
1. Throughput vs. Time: The graph describes throughput in AES algorithm and Onion routing protocol. The throughput in onion routing protocol have been increased when compared to the existing routing protocol [3].

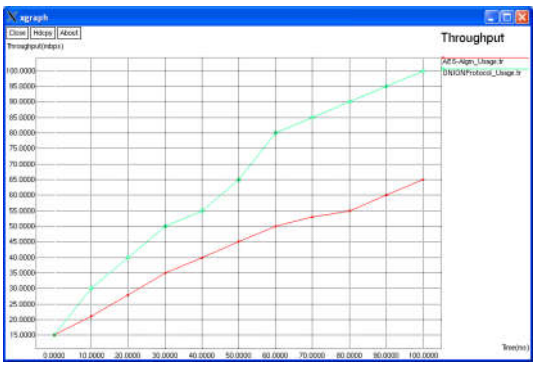

Fig 7 Throughput (Mbps) vs. Time (ms)

End-to-End delay vs. Time: The graph describes end-to-end delay in AES algorithm and Onion routing protocol. The end to end delay in onion routing protocol have been reduced when compared to the existing routing protocol.

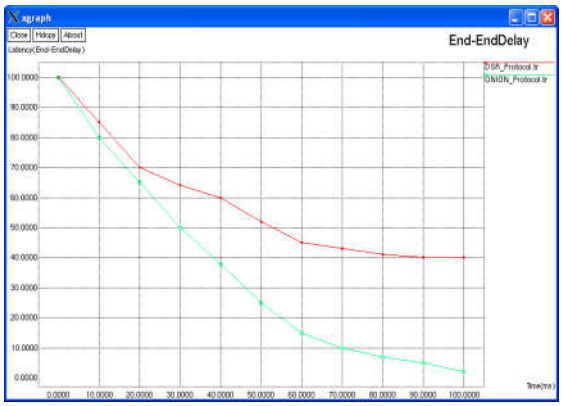

Fig 8 End to end delay vs. Time (ms)

QoS parameters for proposed system: The graph describes different QoS parameters such as packet delivery ratio (PDR), end-to-end delay, throughput and security level.

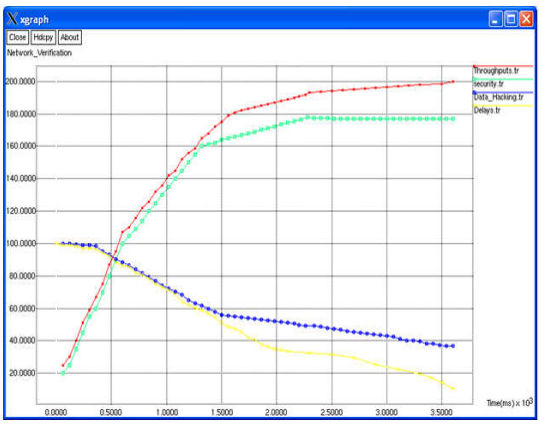

Fig 9 QoS parameters for proposed system

Modern networks contain a variety of middle boxes, whose behavior is affected both by their configuration and by mutable state updated in response to packets received by them. The table 2 describes the parameter constraints in proposed protocol which has high PDR (Packer Delivery Ratio), low end-to-end delay, high throughput and low hacking due to encryption standards used.

Table 2 Comparison of existing protocols with proposed with their parameter constraints

Parameter constrant	Routing protocols in manet	
	AODV	TOP With Storage Constrained QOS
Throughput (Mbps)	75	95
Packet Delivery ratio	0.742	0.815
Average end-to-end delay	20	5

Hence, the results show that there is considerable increase in throughput and decrease in end to end delay due to the combination of capacity constrained QoS protocol and ONION encryption.

CONCLUSION

In this work, we presented security, which can augment most existing reactive routing protocols in MANET to provide reliable and energy-efficient packet delivery against the unreliable wireless links. We introduced a biased back off scheme in the route discovery phase to find a robust virtual path with low overhead. Without utilizing the location information, data packets can still be greedily progressed toward the destination along the virtual path. Secure routing establishes routes that can meet source nodes trust/energy requirements. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. We extended AODV to demonstrate its effectiveness and feasibility. Simulation results showed that, as compared with other protocols, AODV can effectively improve robustness, end-to-end energy efficiency, and latency.

References

1. S.R. Raja and Dr.K.Alagarsamy, "Routing Protocols In Manet Qos Survey," in *International Journal of Innovative Research in Advanced Engineering* (IJIRAE) ISSN: 2349-2163 Issue 5, Volume 2 (May 2015).
2. Chung-Ming Huang, Kun-chan Lan and Chang (November 2008) "A Survey of Opportunistic Networks", Zhou Tsai Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan, R.O.C.
3. C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in Proc. IEEE WMCSA, 1999, pp. 90-100.
4. Essam Natsheh, Adznan Jantan, Sabira Khatun, and Shamala Subramaniam," Adaptive Optimizing of Hello Messages in Wireless Ad-Hoc Networks," in *International Arab Journal of Information Technology*, Vol. 4, No. 3, July 2007.
5. Karumuri.Ashok Kumar, B.Neelima, "Enhanced Onion Routing Framework for MANETs," in *International Journal of Science and Research* (IJSR) ISSN: 2319-7064 Volume 4 Issue 12, December 2015.
6. Vamsi Krishna.Y and Vignesh.S, "Anonymous Routing in Trust Valued MANETs Prior to the Deployment of Onion Routing," in *International Journal of Innovative Research in Science, Engineering and Technology* (An ISO 3297: 2007 Certified Organization) Vol. 5, Special Issue 10, May 2016.
7. Vikas Gupta, Ashok Verma, Ajay Lala and Ashish Chaurasia"Scenario Based Performance and Comparative Simulation Analysis of Routing Protocols in MANET", *in IJCSNS International Journal of Computer Science and Network Security*, VOL.13 No.6, June 2013.

****