INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 773-777
RECEIVED : 25/03/2016. PUBLISHED : 01/04/2016
April 1, 2016

SECURE AND RELIABLE ROUTING USING ONION PROTOCOL

P.Magesh[1] M.Jaya Surenther[2] and G.Nagarajan[3]
[1]Information Technology, S.K.P Engineering College
[2]Information Technology, S.K.P Engineering College
[3]Assistant Professor, Information Technology, S.K.P Engineering College

ABSTRACT

In the routing process malicious nodes can repeatedly break routes. Breaking the routes increases the packet delivery latency. In this system based on request response source selects routing path. After that source hashing neighbor nodes id, data with timestamp. Then it transmits the data to destination using E-STAR protocol. The modification is our implementation. Where we deploy onion protocol. Every node while registering, server will provided with Id, primary key, secondary key and decryption key. Source will find out the optimum path and it will collect primary key of all intermediate node. Data's first encrypted using AES algorithm and then with corresponding primary key of all the hops. This wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. Then collecting its id and secondary key which is transmitted to both source and destination node. Same way all the id's and secondary key are collected and concatenated, so as to verify both source and destination. TPA implementation is also achieved for successful validation of concatenated keys their by reward is provided to the intermediate hops.

Keywords:onion protocol,secure routing,AES algorithm,trusted party auditor,anonymous routing.

1. INTRODUCTION

IN multi hop wireless networks, when a mobile node needs to communicate with a remote destination, it relies on the other nodes to relay the packets. This multi hop packet transmission can extend the network coverage area using limited power and improve area spectral efficiency. In developing and rural areas, the network can be deployed more readily and at low cost.

We consider the civilian applications of multi hop wireless networks, where the nodes have long relation with the network. We also consider heterogeneous multi hop wireless networks (HMWNs), where the nodes' mobility level and hardware/energy resources may vary greatly. HMWNs can implement many useful applications such as data sharing and multimedia data transmission.

For example, users in one area (residential neighborhood, university campus, etc) having different wireless-enabled devices (PDAs, laptops, tablets, cell phones, etc.) can establish a network to communicate, distribute files, and share information. In military and disaster-recovery applications, the nodes' behavior is highly predictable because the network is closed and the nodes are controlled by one authority. The nodes are typically autonomous and self-interested and may belong to different authorities.

The nodes also have different hardware and energy capabilities and may pursue different goals. In addition, malfunctioned nodes frequently drop packets and break routes due to faulty hardware or software, and malicious nodes actively break routes to disrupt data transmission. Since the mobile nodes are battery driven and one of the major sources of energy consumption is radio transmission, selfish nodes are unwilling to lose their battery energy in relaying other users' packets. When more nodes are cooperative in relaying packets, the routes are shorter, the network connectivity is more, and the possibility of network partition is lower.

2 RELATED WORKS

2.1 Reputation-Based Schemes Reputation-based schemes [3] attempt to identify the malicious nodes that drop packets with a rate more than a pre- defined threshold in order to avoid them in routing. When a node N A sends a packet to the next node in the routeto relay to N C;N A has to overhear the channel to check whether N B forwards the packet.N A increases the reputation value of N B when it observes a packet transmission; otherwise, it decreases the reputation value of N B. Once the reputation value degrades to a threshold, N A identifies N B as malicious. However, there are a number of situations at which monitoring by overhearing the medium does not work:

1) when a node N B relays a packet to N C, it is possible that N A can- not overhear the transmission due to another concurrent transmission in N A's neighborhood; and

2) if N B is closer to N A than N C;N B could save its energy and circumvent the scheme by adjusting its transmission power to be over- heard by N A but less than the required power for reaching the true recipient N C. In order to reduce the false accusations, the schemes should use tolerant thresholds to guarantee that a node's packet dropping rate can only reach the threshold if the node is malicious. Reputation-based schemes may identify the black-hole attackers that drop all the packets they are supposed to relay. However, they are less effective in detecting the grayhole attackers that drop a portion of the packets. There is an unavoidable tradeoff between missed detections and false accusations. This is because determining an optimal thresh- old that can precisely differentiate between the honest and the malicious nodes is a challenge, especially in HMWNs

2.2 Payment Schemes: Payment (or incentive) schemes use credits (or micropayment) to encourage the nodes to relay others' packets [5]. Since relaying packets consumes energy and other resources, packet relaying is treated as a service which can be charged. The nodes earn credits for relaying others' packets and spend them to get their packets delivered. However, the receipts overwhelm the network because one receipt is composed for each message. To reduce the receipts' number, PIS generates a fixed size receipt per route regardless of the number of messages. In ESIP, the payment scheme uses a communication protocol that can transfer messages from the source node to the destination with limited use of the public key cryptography operations. Public key cryptography is used for only one packet and the efficient hashing operations are used in next packets. Unlike ESIP that aims to transfer messages efficiently, E-STAR aims to establish stable and reliable routes. Although the proposed communication protocol in can be used with E-STAR, we use a simple protocol due to space limitation and to focus on our contributions

3 PROPOSED

3.1 Characteristics of Wireless Communication System. One of the major challenges in ad hoc networks security is that ad hoc networks typically lack of a fixed infrastructure both in form of physical infrastructure such as routers, servers and stable communication links and in the form of an organizational or administrative infrastructure. Another difficulty lies in the highly dynamic nature of ad hoc networks since new nodes can join and leave the network at any time. The major problem in providing security services in such infrastructure-less networks lies on how to manage the cryptographic keys that are needed. When designing protocols for ad hoc networks, whether routing protocols or security protocols, it is important to consider the characteristics of the network and realize that there are many "flavours" of ad hoc networks. Ad hoc wireless networks generally have the following characteristics. This may limit the number and size of messages sent during protocol execution. Energy constrained nodes: Nodes in ad hoc networks will most often rely on batteries as their power source. The use of wireless communication and the exposure of the network nodes increase the possibility of attacks against the network. Due to the mobility of the nodes the risk of them being physically compromised by theft, loss or other means will probably be greater than that for traditional network nodes. In many cases the nodes of ad hoc network may also have limited CPU performance and memory, e.g. low-end devices such as PDA's, cellular phones and embedded devices. As a result certain algorithms that are computationally or memory expensive might not be applicable.

4. MODULES

4.1 NETWORK CONSTRUCTION

In this Project concept, first we have to construct a network which consists of 'n' number of Nodes. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, we can assume that the nodes are moving across the network. Network is used to store all the Nodes information like Node Id and other information. Each node is having primary key, secondary key and private key. Also network will monitor all the Nodes Communication for security purpose.

4.2ROUTE REQUEST BASED ON ROUTING TABLE CHECKING

In this module, source node sends hello interval request to all intermediate nodes for identifying minimum hop count, capacity of intermediate nodes, based on node connectivity. It can use the routing table in the RREQ packet to estimate how many its neighbors have not been covered by the RREQ packet from previous intermediate node. Each intermediate node validates the RREQ packet and updates its routing tables. Finally RREQ reaches to destination node.

4.3ROUTE SELECTION AND SOURCE SIDE ENCRYPTION PROCESS

In this module, the RREQ is received and verified by the destination node. The destination node selects the route based on hop count and throughput. Then the destination node assembles an RREP packet and broadcasts it back to the source node. Each intermediate node validates the RRES 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. Although source conducts the encryption process based on selected route public keys using AASR protocol based on onion routing.

4.4PACKET FORWARDING

In this module, source node forwards the encrypted packet to neighbor node based on selected route. Neighbor node gives it own private key for one part of decryption process. After that it will send to next neighbor node. Similarly each neighbor nodes in selected route decrypts the packet based on its private key using AASR protocol. Sometime attacker node also receives the packets. In that time, it gives its private key but packet is not decrypted. So it didn't analyzes how many number of encryptions placed on. Thus we improve the data security.

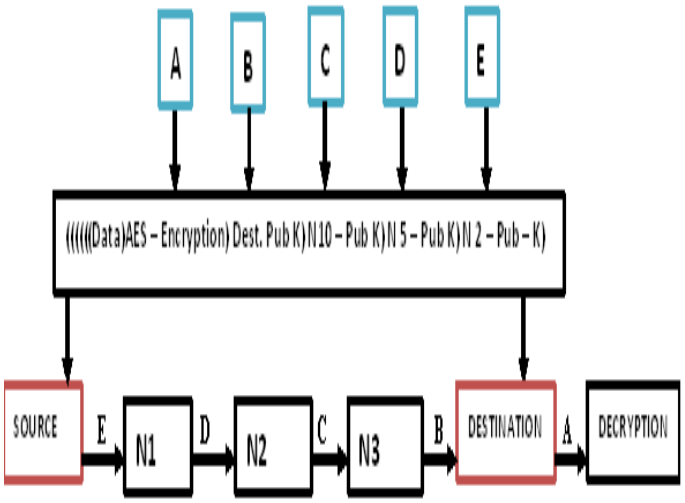
4.5DECRYPTION PROCESS

In this module, neighbor node decrypts the packet and finally sends to destination node. Then the destination node decrypts the packet with its private key and AES decryption key. Finally destination node views the original data. Since the paths capacity will vary dynamically, so that the paths will be changed dynamically as per data transfer along the network. So it increases the packet delivery ratio and decreases the average end-to-end delay.

4.6TPA VERIFICATION AND PAYMENT PROCESS

In this module, after data transmission each intermediate node in selected path sends its id and secondary key to trusted party auditor. Destination node also sends the id and secondary keys of selected nodes to TPA after data retrieval from source node. Then TPA audits the both id and secondary keys are match or not based on ESTAR protocol. If match means TPA rewards to that trusted node. Suppose it mismatch it easily identify the attacker node.

ARCHITECTURE DIAGRAM



CONCLUSION

We have proposed E-STAR that uses payment/trust systems with trust-based and energy aware routing protocol to establish stable/reliable routes in HMWNs. E-STAR stimulates the nodes not only to relay others' packets but also to maintain the route stability. It also punishes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. We have proposed SRR and BAR routing protocols and evaluated them in terms of overhead and route stability. Our protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the nodes' past behavior, and the route lifetime based on the nodes' energy capability. SRR 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. For BAR, destination nodes establish the most reliable routes but with more overhead comparing to SRR. The analytical results have demonstrated that E-STAR cansecure the payment and trust calculation without false accusations. Moreover, the simulation results have demonstrated that E-STAR can improve the packet delivery ratio due to establishing stable routes.

REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom'00, pp. 255-265, Aug. 2000.

[4] K. Liu, J. Deng, and K. Balakrishnan, "An Acknowledgement- Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.

[5] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE. INFOCOM '03, vol. 3, pp. 1987-1997, Mar./ Apr. 2003

AUTHORS

	M.Jaya Surenther Information Technology S.K.P Engineering College Tiruvannamalai		P.Magesh Information Technology S.K.P Engineering College Tiruvannamalai