isrjournals

International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 1 Apr,2016,ISSN_NO: 2320-7248

Secure Interhop Reliable Routing

J.Asha*,P.Deepika*,S.Dhivya*, S.Famitha

*(Assistant Professor-II), Computer Science And Enginerring ,
Prathyusha Engineering College, India.
ashajanakiraman@gmail.com

.

ABSTRACT— Onion protocol is a layered protocol for reliable routing. The aim of onion protocol is to improve security and reduce the packet delay. In this every node while registering, the server provides 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 is encrypted with AES algorithm and then with the corresponding primary key of all 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— Securing heterogenous multihop wireless network,packet dropping and selfishness attacks,trust systems and secure routing protocols.

1. INTRODUCTION

In the existing system malicious nodes can repeatedly break routes. Breaking the routes increases the packet delivery latency. The multi hop packet transmission can extend the network coverage area. Due to the multi hop packet transmission, node's mobility level and hardware/energy resources may vary greatly. The main disadvantage is Waiting time is increased because the shortest path cannot be determined by the system. The data transmission rate is also less due to long path. Since the transaction time is long we cannot guaranty the security of the internet packet so it provides less security.

Volume: 2 Issue: 1 Apr,2016,ISSN_NO: 2320-7248

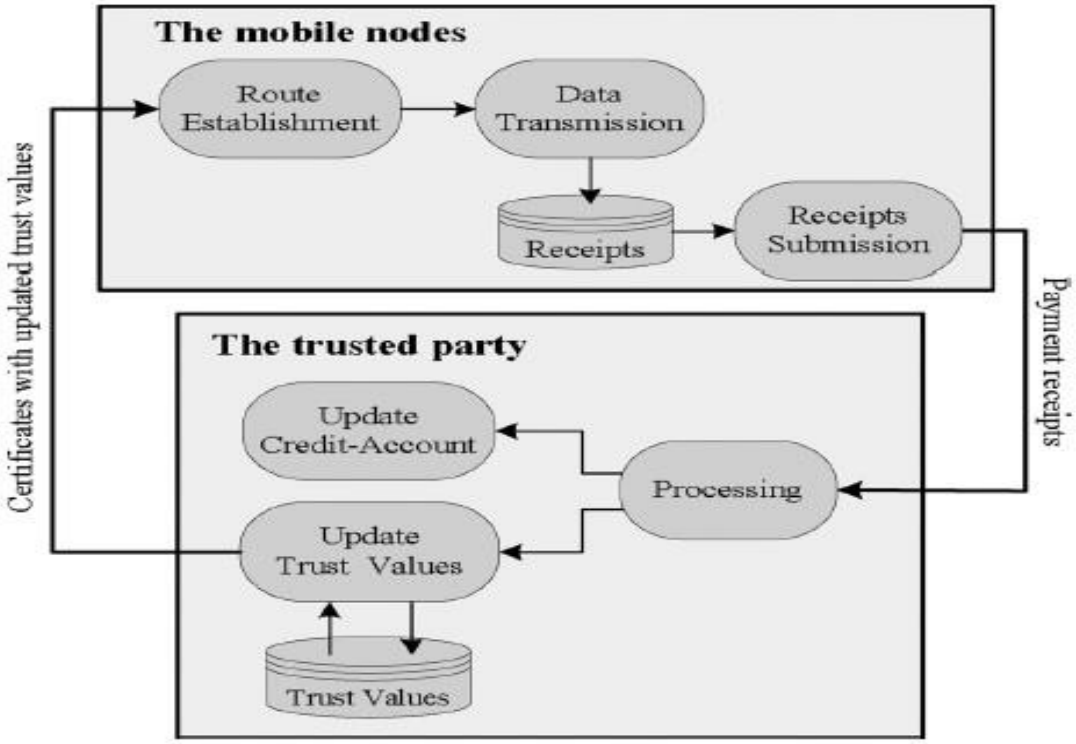

Fig 1.System architecture for Existing System

2. PROPOSED SYSTEM:

In proposed system, onion protocol is used. Based on request response source selects routing path. Every node while registering, server will provided with primary key, id, secondary key and decryption key. Data is encrypted with primary key of all hops. This wholesome is transmitted to first hop. Then id and secondary key is transmitted to both source and destination node and it is collected and concatenated, so as to verify both source and destination. The advantage of proposed system is waiting time is decreased by finding the shortest route. And the system is made reliable with more data transmission rate at high security.

3. ARCHITECTURE DIAGRAM:

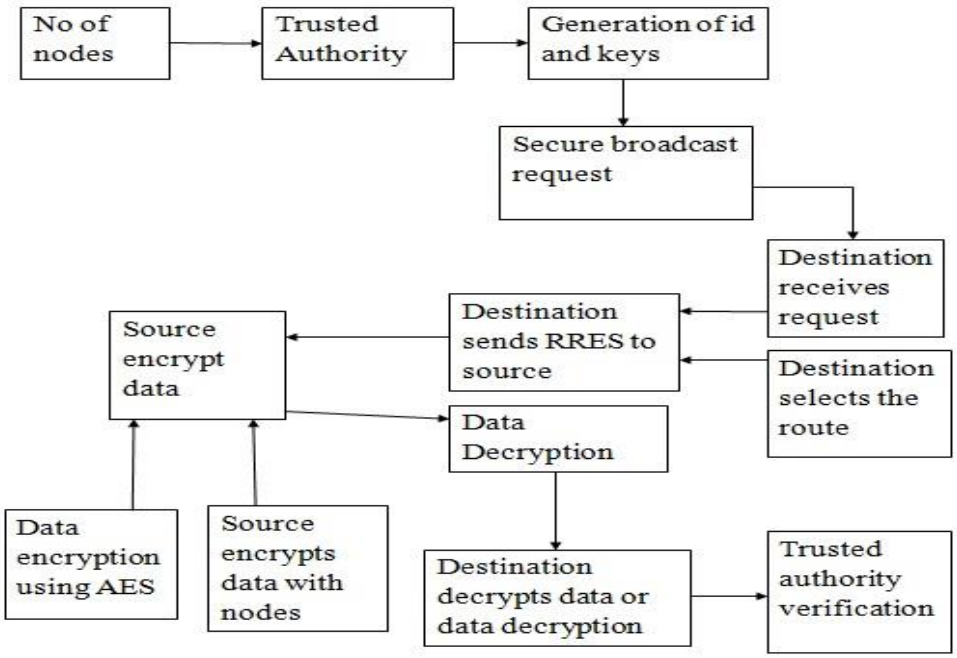

Fig 2. System Architecture for proposed system

4. ALGORITHM:

AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits

5. 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.

6. ROUTE 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.

7. ROUTE 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

8. PACKET 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. Some time 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.

9. DECRYPTION 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.

10. TPA 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.

11. 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 can secure 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.

12. FUTURE ENHANCEMENT:

To ensure Data security and privacy data is spitted into multiple block encrypted and stored in multiple images to ensure security.

REFERENCES

[1] Performance evaluation of on demand routing protocols aodv and modified adov (R-ADOV) in manets,Humaira Nishal,vol 2,Jan 2014.

[2] An efficient secure distributed anonymous routing protocol for mobile and wireless ad-hoc networks,Azzedine Boukerche,vol 29,21 july 2012.

[3] Secure neighbor discovery system for ad-hoc through AASR protocol,international journal of computer science information and technology and security,ISSN:2249-9555,vol 4,no 6,Dec 2014.

[4] Anonymous on-demand routing in mobile ad-hoc networks,Jiejung Kong,Xiaoyan Hong,Mario Gerla,University Of California,Los Angeles,CA 90095.

[5] Anonymous secure communication in wireless mobile ad-hoc networks,SK.MD Mizanur Rahman,vol 25,no 1,May 2007.

[6] An identity-free and on demand routing scheme against anonymity threats in mobile ad-hoc networks,Liaoyan Hong,scalable network technologies,Inc 6701 centre drive west,Nov 2011.

[7] Trust Management in Distributed Systems,H.Li and M.Singhal,Computer, vol. 40, no. 2, pp. 45-53, Feb. 2007.

[8] Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,S.Marti,T.Gjuli, Proc. ACM MobiCom'00, pp. 255-265, Aug. 2000.