International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 1, March-May, 2017 | Pages 59-65

Secure Onion: Secure Inter Hop Verification with Onion Protocol Implementation for Reliable Routing in Wireless Sensor Networks

Bimal Kalsa, P.Sathish Kumar, R.ArumugaArun[1]
[1]Assistant Professor, Loyola Institute of technology, Chennai, India
M. Boopathi Raja, K.Swathi[2]
[2]Associate Professor, Loyola Institute of technology, Chennai, India
[1]Corresponding Author: E-mail:kalsaalex@gmail.com

Abstract: In the existing system, malicious nodes can repeatedly break routes. Breaking the routes increases the packet delivery latency. In the Proposed 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. In the modification process, 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 – AES Algorithm, E-Star Protocol

ABSTRACT

In the existing system, malicious nodes can repeatedly break routes. Breaking the routes increases the packet delivery latency. In the Proposed 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. In the MODIFICATION PROCESS, 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.

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.

However, the nodes' behavior is unpredictable in civilian applications for different reasons. 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. Moreover, since the nodes are equipped with different hardware capability, such as CPU speed and buffer size, the nodes having large hardware resources can perform packet relay more successfully than others. For example, PDAs may not be able to relay packets effectively due to the scarcity of resources. In HMWNs, a route is broken when an intermediate node moves out of the radio range of its neighbors in the route. In addition, some nodes may break routes because they do not have sufficient energy to relay the source nodes' packets and keep the routes connected. Because of this uncertainty in the nodes' behavior, randomly selecting the intermediate nodes will degrade the routes' stability.

It will also endanger the reliability of data transmission and degrade the network performance in terms of packet delivery ratio (PDR). Only one intermediate node can break a route, and a small number of incompetent or malicious nodes can repeatedly break routes. When a route is broken, the nodes have to rely on cycles of time-out and route discoveries to re-establish the route. These route discoveries may incur network-wide flooding of routing requests that consume a substantial amount of the network's resources. Breaking the routes increases the packet delivery latency and may cause network partitioning and the multi-hop communication to fail. Hence, in order to establish stable routes and maintain continuous traffic flow, it is essential to assess the nodes'

2. RELATED WORK

Prior work on privacy aspects of telematics and location-based applications has mostly focused on a policy-based approach . Data subjects need to evaluate and choose privacy policies offered by the service provider. These policies serve as a contractual agreement about which data can be collected, for what purpose the data can be used, and how it can be distributed. Typically, the data subject has to trust

the service provider that private data is adequately protected. In contrast, the anonymity-based approach de-personalizes data before collection, thus detailed privacy-policies and safeguards for data are not critical.

2.1 EXISTING SYSTEM

In the existing system, malicious nodes can repeatedly break routes. Breaking the routes increases the packet delivery latency

3. EXPERIMENTAL WORK

3.1 PROPOSED SYSTEM

In the PROPOSED 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.

.

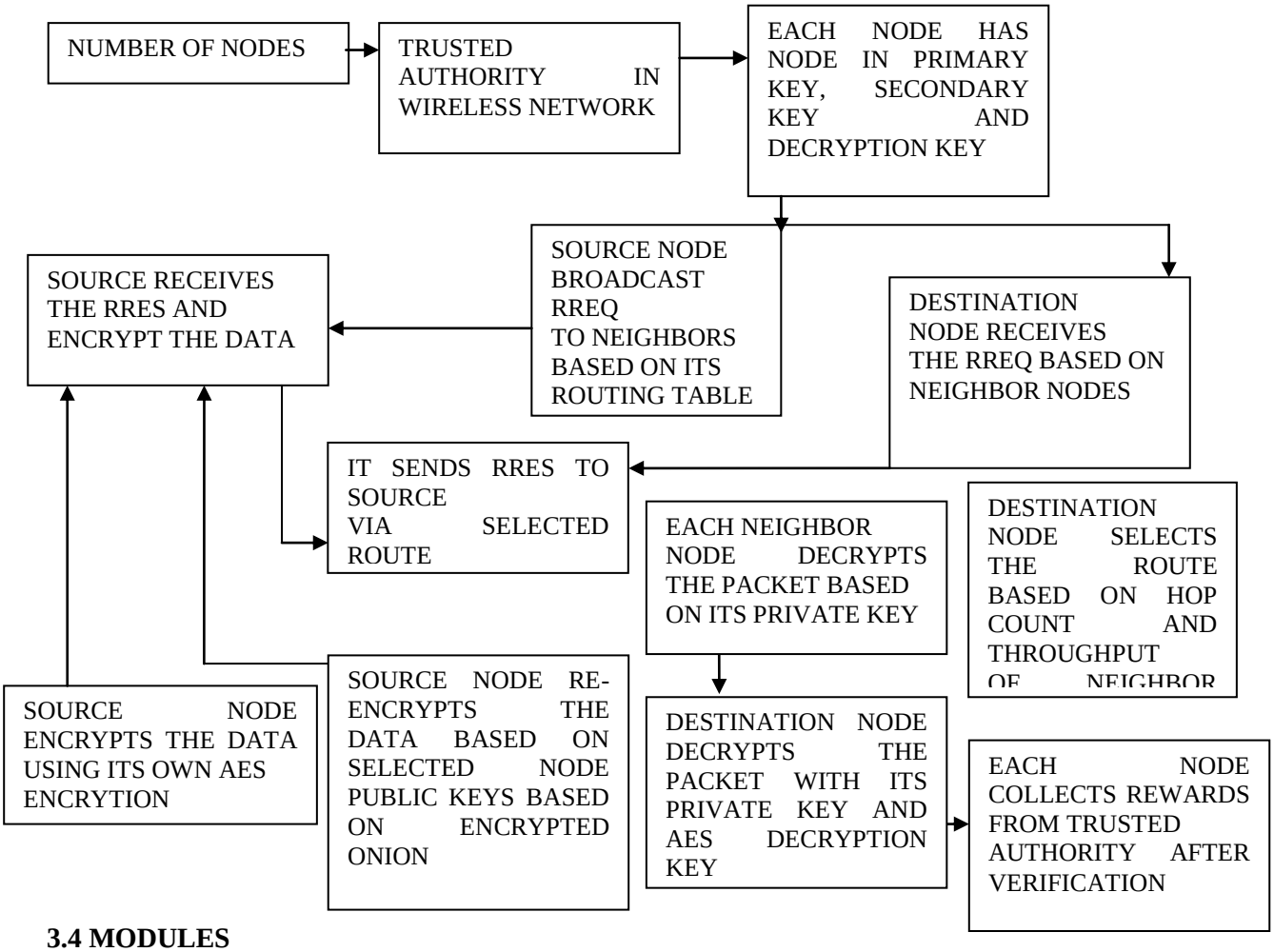
2.2 ALGORITHM

AES Algorithm competence and reliability in relaying packets to make informed routing decisions. In this paper, we propose E-STAR, a secure protocol for Establishing Stable and reliable Routes in HMWNs. E-STAR integrates trust and payment systems with a trust-based and energy-aware routing protocol. The payment system uses credits (or micropayment) to charge the nodes that send packets and reward those relaying packets. Since a trusted party (TP) may not be involved in the communication sessions, an offline trusted party is required to manage the nodes' credit accounts. The nodes compose proofs of relaying packets, called receipts, and submit them to TP. The payment system can stimulate the selfish nodes to relay others' packets to earn credits. It can also enforce fairness by rewarding the nodes that relay more packets such as those at the network center. However, the payment system is not sufficient to ensure route stability. It can stimulate the rational nodes to not break routes to earn credits, but the routes can be broken due to other reasons. Specifically, the IETF Geopriv working group is addressing privacy and security issues regarding the transfer of high resolution location information to external services and the storage at location servers. It concentrates on the design of protocols and APIs that enable devices to communicate their location in a confidential and integrity-preserving manner to a location server. The location server can reduce the data's resolution or transform it to different data formats, which can be accessed by external services if the data subject's privacy policy permits. The working group is also interested in enabling unidentified or pseudonymous transfer of location information to the server and access from the server. However, it does not claim that this provides a sufficient degree of anonymity.

3.2.1. AES ALGORITHM

Advanced Encryption Standard, AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Most AES calculations are done in a 2 special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. Each each containing four similar but different stages, including one that depends on the encryption key itself.

3.3 SYSTEM ARCHITECTURE



3.4 MODULES

1. NETWORK CONSTRUCTION
2. ROUTE REQUEST BASED ON ROUTING TABLE CHECKING
3. ROUTE SELECTION AND SOURCE SIDE ENCRYPTION PROCESS
4. PACKET FORWARDING
5. DECRYPTION PROCESS
6. TPA VERIFICATION AND PAYMENT PROCESS

MODULES DESCRIPTION

3.4.1 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.

3.4.2 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.

3.4.3 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.

3.4.4 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. 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.

3.4.5 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.

3.4.6 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.

4.FUTURE WORK

In response to the problems that the current Internet is facing, a number of research initiatives were started with the goal of defining new network architectures for the next-generation

Some of the new architectures that have been proposed already include features which can be leveraged by anonymity networks (though the reason for their inclusion in the design lies strictly in networking

aspects). In particular, some of these FIAs grant the end hosts a certain degree of control over the path that their traffic takes to tra-verse the network . Control, or at least knowlege of the path, is typically offered at the granularity of Autonomous Systems (ASes) or Internet Service Providers (ISPs). Assuming that the ISPs and ASes have public cryptographic keys that can be obtained and verified by the source, it is even possible for the source to negotiate keys with the nodes on the path to perform cryptographic operations on packets, (e.g., onion encryption).

5.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.

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] X. Li, Z. Li, M. Stojmenovic, V. Narasimhan, and A. Nayak, "Autoregressive Trust Management in Wireless Ad Hoc Networks," Ad Hoc & Sensor Wireless Networks, vol. 16, no. 1-3, pp. 229-242, 2012.
[5] G. Indirania and K. Selvakumara, "A Swarm-Based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)," Int'l J. Parallel, Emergent and Distributed Systems, vol. 29, pp. 90-103, 2014.
[6] H. Li and M. Singhal, "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45-53, Feb. 2007.
[7] 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.
[8] 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.