Indian Journal of Emerging Electronics in Computer Communications
Vol.3, Issue 2 (2016) Page.588-595
ISSN: 2393-8366

Secure Onion Protocol Implementation for Reliable Routing in Wireless Sensor Networks

Mighty Ecclisha M[1], Jisha Liju Daniel[2], S. Brindha[3]
[1]*Research Scholar, St.Peter's University, Chennai.*
mecclishamagi@yahoo.in
[2]*Asst.Prof. & Dept. of Computer Science & Applications, St.Peter's University, Chennai*
[3] *Asst.Prof. & Dept. of Computer Science & Applications, St.Peter's University, Chennai*

***Abstract**-- In this paper, we propose secure onion protocol implementation for reliable routing in wireless sensor networks. Deploy onion protocol is implemented using AES algorithm and with corresponding primary key of all the hops. 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, TPA, Onion Protocol*

I. INTRODUCTION

Mobile Adhoc Network (MANET) is using a temporary network communication they do not have any central administration and existing infrastructure. So nodes in wireless network dynamically form their own network. Wireless network nodes use some default routing protocols to identify the sender and receiver for every message and network security is a major issue. Over some years, more number of networks has been proposed with onion routing technique and some networks have been implemented. Onion routing, is a technique where message are covered in multiple encryption layers, forming an encryption like onion. In this scheme delivering message to destination by a no of intermediate onion nodes or routers, each intermediate router and node is responsible to decrypt one layer, and forward the packet or message to next router or node. In onion routing scheme they randomly select a path over the onion routers network and form a circuit. After formed the circuit, each nodes in the circuit shares symmetric to user, that key will be used to encrypt future onion layers. In this proposed system we present onion routing protocol and Advanced Encryption technique. In that First network is constructed with n no of nodes. After that nodes in the network can request data packet to other nodes. We can simulate nodes in the networks are moving because of the nodes mobility property. All nodes are maintained to forward data packet to other nodes. In this proposed scheme, discovering the shortest path is first process, and sends the packets to other node. When nodes come for registering into to the network, they get id and other information.

In this multi hop route forwarding is used to identify shortest path detection and Advanced Encryption Standard algorithm is used to achieve encryption process. Data is encrypted using Advanced Encryption Standard (AES) technique with primary key of all intermediate nodes. The wholesome is forwarded to first node, where the first decryption will be done by that node decryption key.In this proposed system, source node transmits the encrypted data packet to intermediate node depending on the selected route. Then intermediate nodes decrypt and transmit packet to destination node. Finally destination nodes get data securely by its last decryption process. Using this system we achieve the data forwarding securely and shortest way. This system mainly overcomes the problems of Existing Electronic Suspense Tracking and Routing (ESTAR) system, which ensure route stability, malicious, selfish attacks, and node failure. This proposed system use new protocol with encryption for packet delivery speed and most secure data forwarding.

II. MATERIAL AND METHODS

This paper proposes onion routing protocol with Advanced Encryption Standard and multi hop route forward algorithm. By implementing onion protocol every node while registering, server will be provided with Id, primary key, secondary key and decryption key. This system provides a very securable and fast reliable packet delivery. Source will find out the optimum path and it will collect primary key of all intermediate node. First we need to construct the network with n number of nodes. After that nodes can forward data from one to other node in that network. Nodes in the network are moving, because it's having the mobility property.

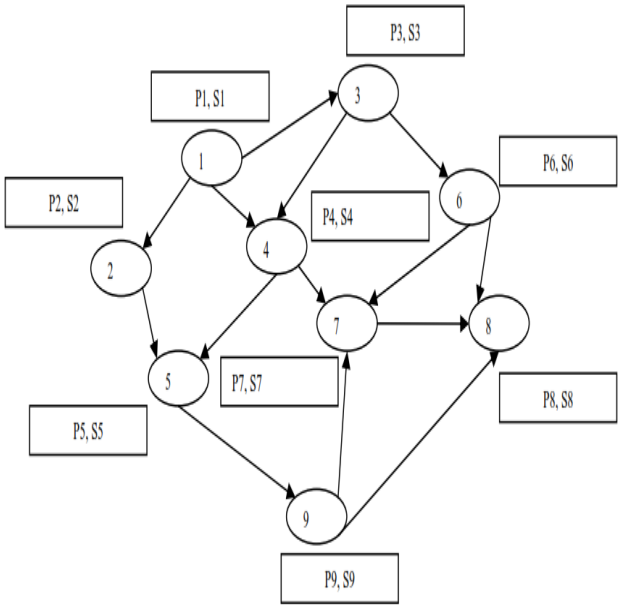

Fig 1. Network construction

The networks gets node id, primary and secondary key once nodes enter into the network. Nodes primary and secondary keys are used to encryption and decryption operation. MANET is a collection of mobile devices with wireless connectivity. It has no fixed infrastructure, restricted resources and broadcast range. Communication between the nodes is achieved by the dynamically discovered routes but identifying the routes between nodes is major task. The security and efficiency

is an important concern while forwarding the packet. By using multi hop route forwarding algorithm to discover the shortest path from source to destination. After finding routes between source and destination, Source sends packet to destination. This protocol is used to provide security on data by some layer of encryption, and it overcomes the packet delay latency. Normally nodes in the multi-hop wireless networks would like to communicate with other nodes in networks; so it can transmit the packet by the help of other nodes in the network. This type of multi hop packet transmission is able to extend the network coverage area by spectral efficiency of area and limited power this multi hop networks can be used in rural and developing areas at low cost in is more readily available. When consider the multi hop wireless civilian networks, nodes in network contains the long connection with network.

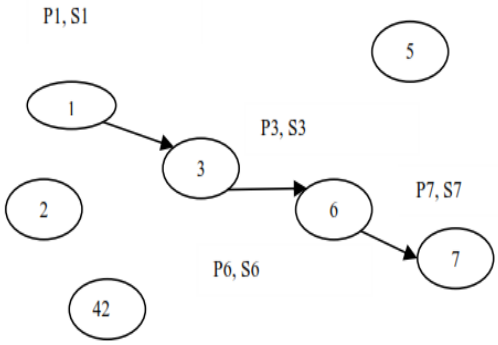

Fig 2. Shortest Route Discoveries from Source to Destination

For various reasons Sometimes behaviours of node is unpredictable in the application of civilians. The nodes may be self-interested and autonomous and it belongs to different authority. The nodes have different energy capabilities and hardware and may have various goals. Malfunctioned and selfish node is the addition problem in mobile network. Because of malfunctioned nodes drop the packets frequently and break the routes due to the software and hardware problems and this type nodes disrupts the transmission of data. Since mobile nodes are running in battery driven, some nodes are not interest to transmit the packets to save their energy. Due to this nodes uncertainty behaviour, dynamic routes will degrade stability of routes. It is also one of the reasons to endanger the data transmission reliability and degrade the performance of network. In wireless network one node could be a reason to break route, and some selfish or malicious nodes can break the routes repeatedly. If any route is broken when transmitting the packet to other nodes, the node has to retransmit the packet and identify the new route. Route breaking increases the delivery latency of packet and may reason communication fail in multi-hop. In order to create stable route to transmit packet and maintain the traffic flow, considering the nodes ability and reliability takes places to create informed routing decisions. Once the shortest path is discovered successfully from source to destination, Source node collects primary key of all intermediate nodes. Then source node start the first encryption process by the destination node primary key. Respectively, the encryption process is done by all intermediate nodes primary keys. Source node forwards the encrypted packet to neighbor or intermediate node based on selected route. Neighbor node provides secondary key for decryption process and decrypt the data. After that the neighbor node forwards the data packet to next intermediate node. Like that all the neighbor nodes in the selected route are decrypted by its secondary key. Finally destination nodes receive the secured and reliable data packet by its decryption process.

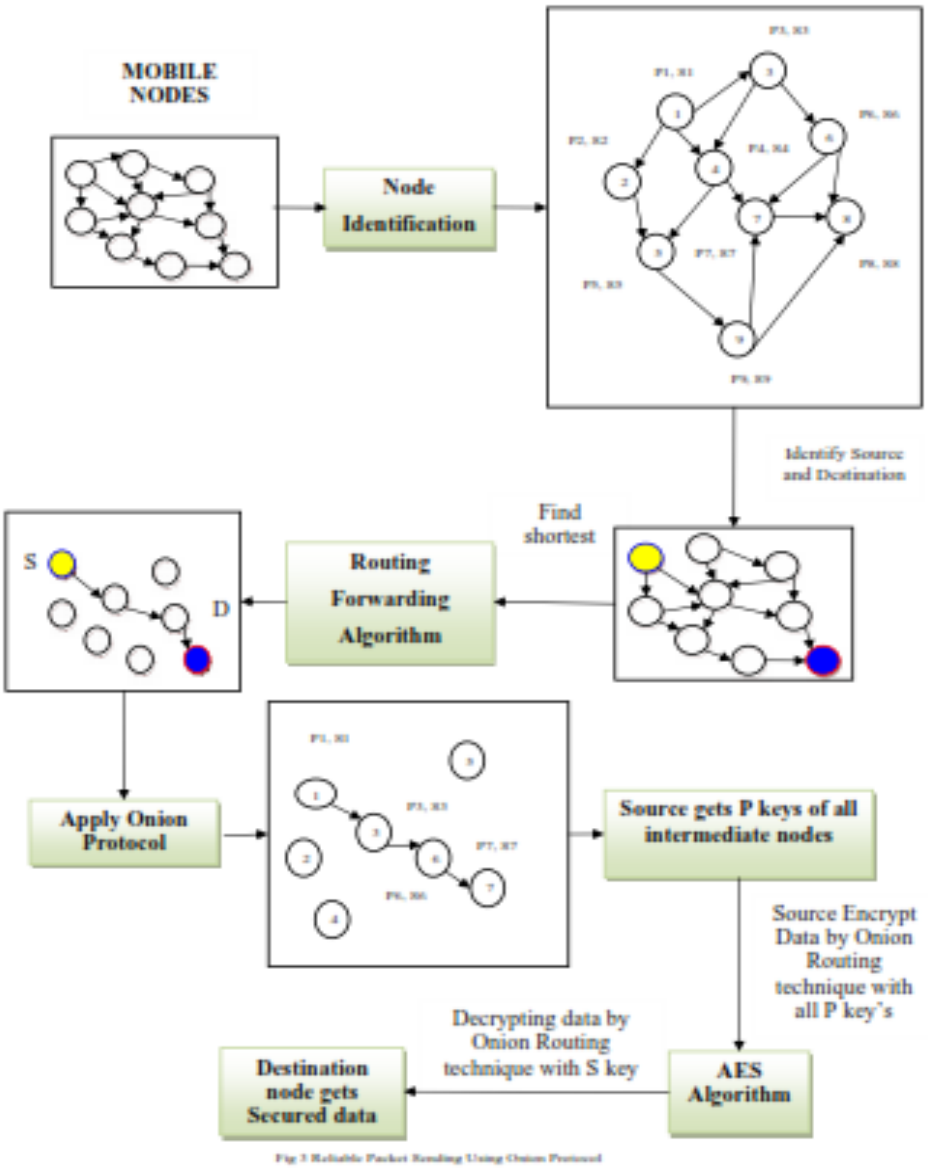

Fig 3. Reliable packet sending using onion protocol

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. 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. In packet forwarding, 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. In decryption process, 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. In TPA verification and payment process, 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.

A. RESULTS

This paper proposes Advanced Encryption Standard with onion protocol to overcome the issues of Electronic Suspense Tracking and Routing (E-STAR) protocol, and we use multi hop route forward algorithm to select the shortest path from source to destination. The First process of this paper is constructing the network with n number of nodes. Network construction with n number of nodes. Constructing the network is used to relay the data packet from one node to other node in the network. The process of nodes getting its node id, primary and secondary key. These two key are used to perform the encryption and decryption operation on data packet. In the proposed system multi hop route forwarding algorithm is used to find the shortest path from source to destination. Finding the route is important to forward the packet from one node to another. In existing system Electronic Suspense Tracking and Routing (E-STAR) protocol is used to transmit the packet with secure and reliable way. It used the reward and the below table shows the node execution time from source node to destination node. When compared to existing system our proposed system minimize time for nodes to reach the destination. This system also support, if number of nodes increases in intermediate path in network, it will reach the destination more quickly than existing system.

No. of Nodes	E-Star	Onion Protocol
10	30.984	10.967
20	40.125	20.963
30	60.324	40.734
40	110.871	90.576

Table 1. Packet reaching time from destination

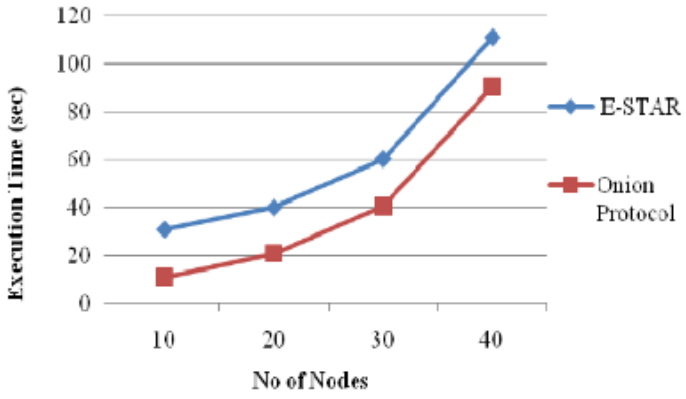

Fig 4. Packet reaching time from source to destination

The advantages of proposed system are less waiting time, reliable, high data transmission rate, more effective and highly secure.

III DISCUSSION

In HMWNs, nodes are not able to transmit the packet to other effectively due to nodes moving from transmission range to neighbor transmission range. Due to this nodes uncertainty behaviour, dynamic routes will degrade stability of routes. It is also one of the reasons to endanger the data transmission reliability and degrade the performance of network. In wireless network one node could be a reason to break route, and some selfish or malicious nodes can break the routes repeatedly. If any route is broken when transmitting the packet to other nodes, the node has to retransmit the packet and identify the new route. These types of route discoveries may bring network wide flooding of routing request that takes a more amount of network resources. For various reasons Sometimes behaviours of node is unpredictable in the application of civilians. The nodes may be self-interested and autonomous and it belongs to different authority. The nodes have different energy capabilities and hardware and may have various goals. Malfunctioned and selfish node is the addition problem in mobile network. Because of malfunctioned nodes drop the packets frequently and break the routes due to the software and hardware problems and this type nodes disrupts the transmission of data. Since mobile nodes are running in battery driven, some nodes are not interest to transmit the packets to save their energy. When many nodes are in cooperative mode to relay the packets, the routers will be short, and network connectivity, network partition possibility is lower. Moreover nodes in the network have equipped with different hardware quality, such as buffer size and CPU speed, the nodes whose having more hardware resources can easily perform packet transmission more successfully when compared to other nodes. In existing system Electronic Suspense Tracking and Routing System (E-STAR) protocol is used to establish a reliable and stable routes in Heterogeneous multi hop wireless networks. Electronic Suspense Tracking and Routing System (E-STAR) combines payment and trust systems with an energy-aware and trust-based routing protocol. However, this payment system will not sufficiently ensure the stability of route. In the proposed system it use stimulate method for nodes to avoid the route break to earn credits, but due to some other reasons routes could be broken.

Example of some reasons includes node failure, low resources, and selfish attacks. To overcome these issues we use onion routing protocol with Advanced Encryption Standard and multi hop routing algorithm. This proposed system provides reliable and secure packet forwarding mechanism. TPA implementation is also achieved for successful validation of concatenated keys their by reward is provided to the intermediate hops.

IV CONCLUSION

In existing system E-STAR that uses payment/trust systems with trust-based and energy-aware routing protocol for stable routes. 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. In proposed system we use onion routing protocol for secure and reliable packet transmission. Onion protocol provides the layer of encryption and decryption process to secure the packet while transmitting to destination node and this system uses the multi hop route forwarding algorithm to find the shortest path from source to destination. Onion protocol with Advanced Encryption Standard algorithm is a two key encryption process. In this source the encrypted data with primary keys and each neighbor node is responsible for decrypting the packet with its secondary key, so any neighbor node in the selected route cannot access the data while transmitting the packet to other neighbor node. When compared to the existing system our proposed system provides more security on data and minimizes the overhead of network. In future enhancement, to ensure Data security and privacy data is spitted into multiple blocks encrypted and stored in multiple images to ensure security.

REFERENCES

[1]Ismail, D, Jaafar, M, (2007), "Mobile ad hoc network overview", Applied Electromagnetics, Asia-Pacific Conference, IEEE , Page 1 - 8 DOI 10.1109/APACE.2007.4603864
[2]Volker Fusenig, Dagmara Spiewak; Engel, T. (2007), "Acimn protocol: A protocol for Anonymous Communication In Multi hop wireless Networks" Wireless Telecommunications Symposium, Pomona, CA, IEEE , DOI: 10.1109/WTS.2007.4563320.
[3]G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, (2009), "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical Journal, vol. 13, no. 4, pp. 175-193.
[4]Ritu Aggarwal, (2013) "Security on Dynamic Source Routing Protocol Using Onion Routing Encryption", International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Volume-2, Issue-6
[5]G. Indirania and K. Selvakumara, (2014), "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.
[6]H. Li and M. Singhal, (2007), "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45-53.
[7]C. Chou, D. Wei, C. Kuo, and K. Naik, (2007), "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE Journal on Selected Areas in Communications, VOL. 25, NO 1.
[8]Volker Fusenig, Dagmara Spiewak; Engel, T. (2007), "Acimn protocol: A protocol for Anonymous Communication in Multi hop

[9]Wireless Networks" Wireless Telecommunications Symposium, Pomona, CA, IEEE , DOI: 10.1109/WTS.2007.4563320.
[10]Vasantha, V., Manimegalai, D., (2007), "Mitigating Routing Misbehaviors Using Subjective Trust Model in Mobile Ad Hoc Networks" Conference on Computational Intelligence and Multimedia Applications International Conference IEEE (Volume:4) Pp.417 - 422
[11]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.
[12]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.
[13]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.
[14]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.