ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

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

S.Ashwini[1], S.Christy Melwyn[2], K.Ravi Kumar[3]

M.E Final year, Dept. of CSE, Rrase College of Engineering, Chennai, India[1]

Assistant Professor, Dept. of CSE, Rrase College of Engineering, Chennai, India[2]

HOD, Dept. of CSE, Rrase College of Engineering, Chennai, India[3]

**ABSTRACT***:* The wireless sensor networks in the inter hop verification could sustain many problems with transformation of data packets so we propose E-STAR for establishing stable and reliable routes in heterogeneous multi hop wireless networks. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. We develop two routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E-STAR can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, for the efficient implementation of the trust system, the trust values are computed by processing the payment receipts. Analytical results demonstrate that E-STAR can secure the payment and trust calculation without false accusations. Simulation results demonstrate that our routing protocols can improve the packet delivery ratio and route stability.

**KEYWORDS**:E-STAR;Trust-based and energy-aware routing protocol;multi-dimensional trust values.

## I. 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 neighbourhood, 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' behaviour is highly predictable because the network is closed and the nodes are controlled by one authority.

## II. RELATED WORKS

The aim of the project is to improve security and to reduce the packet delay based on ESTAR protocol and to prevent data in adversarial environment.A major requirement on the network is to provide unindentifiability and unlinkability for mobile nodes and their traffics. The existing protocols are vulnerable to the attacks of fake routing packets or denial-of-service (DoS) broad casting, the requirement is not fully satisfied.

DOI: 10.15680/IJIRCCE.2016. 0405199

## III. SYSTEM MODEL

The considered HMWN has mobile nodes and offline trusted party whose public key is known to all the nodes. The mobile nodes have different hardware and energy capabilities. The network is used for civilian applications, its lifetime is long, and the nodes have long relation with the network. Thus, with every interaction, there is always an expectation of future reaction. Each node has a unique identity and public/private key pair with a limited-time certificate issued by TP. Without a valid certificate, the node cannot communicate nor act as an intermediate node. TP maintains the nodes' credit accounts and trust values. Each node contacts TP to sub-mit the payment receipts and TP updates the involved nodes' payment accounts and trust values. This contact can occur via cellular networks or Internet.

## IV. PURPOSE AND GOALS

Mobile computing encompasses a number of technologies and devices, such as wireless LANs, notebook computers, cell and smart phones, tablet PCs and PDAs. Basically, any electronic device that helps you organizes your life, communicate with co workers or friends, or do your job more efficiently is part of mobile computing. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the principle of mobile computing.

## V. DESIGN AND IMPLEMENTATION

In the implementation where we deploy onion protocol. Every node while registering, server will provided with Id, primary key, secondary key and decryption key. Sources will findout 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.

## VI. NETWORK SIMULATOR

Network simulator is an object-oriented discrete event simulator. It is also a package of tools that simulates behavior of networks. It is primarily UNIX based. It creates network topologies. It is written in C++ and OTCL formats (TCL scripting with object-oriented extensions). NS is primarily useful for simulating local and wide area networks. It can be used to simulate a variety of IP networks. It implements network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Djikstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN

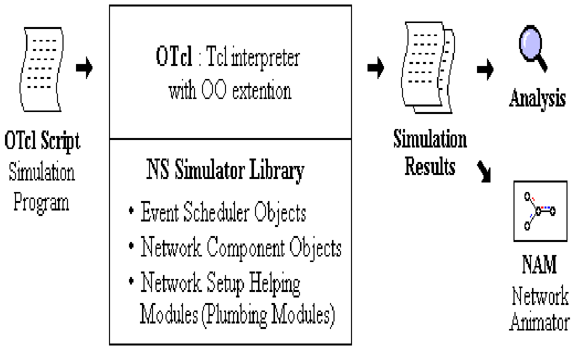

Fig1 representing the NS Simulation in the network.

DOI: 10.15680/IJIRCCE.2016. 0405199

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

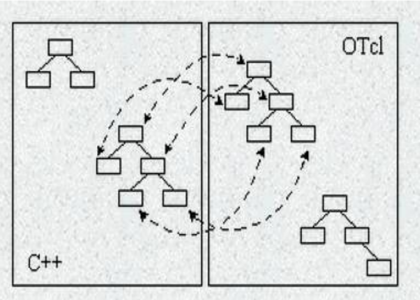

Fig 2 Representing the NS workings in c++,OTcl

NS is written not only in OTCL but in C++ also. For efficiency reason, NS separates the data path implementation from control path implementations. In order to reduce packet and event processing time (not simulation time), the event scheduler and the basic network component objects in the data path are written and compiled using C++. Likewise, an object (not in the data path) can be entirely implemented in OTCL. It shows an object hierarchy example in C++ and OTCL.

## VII. IMPLEMENTATION 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. Sources will findout 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.

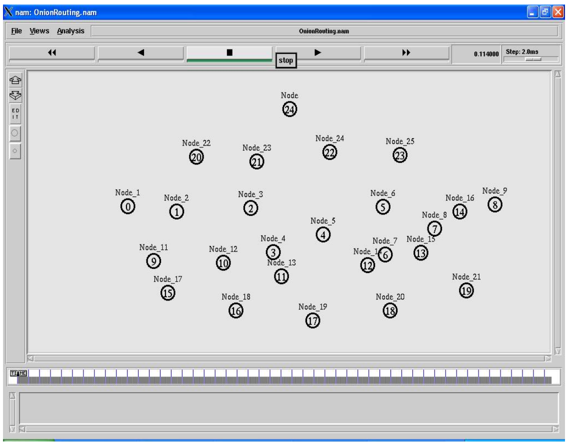

Fig 1 Creating nodes in the network

DOI: 10.15680/IJIRCCE.2016. 0405199

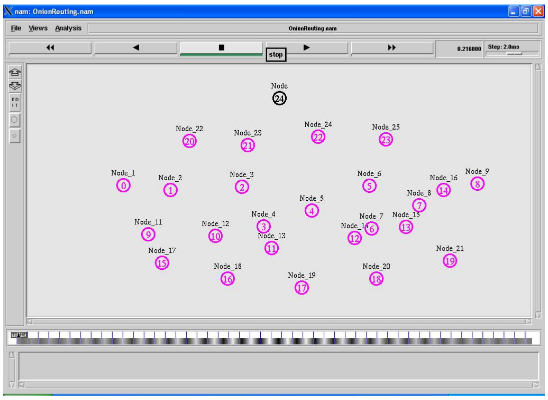

Fig 3 Finding the range and checking the authority  of node to comm.

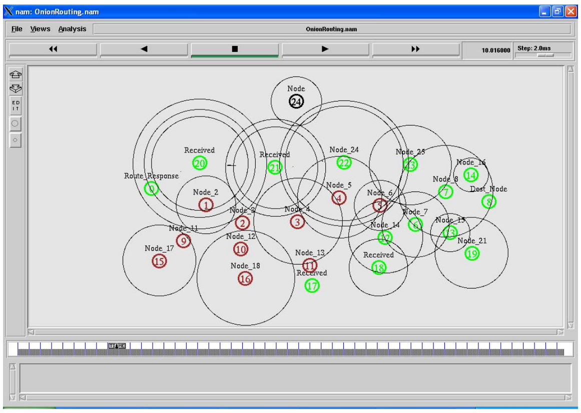

Fig 2 Selecting the path of the data to be travelled

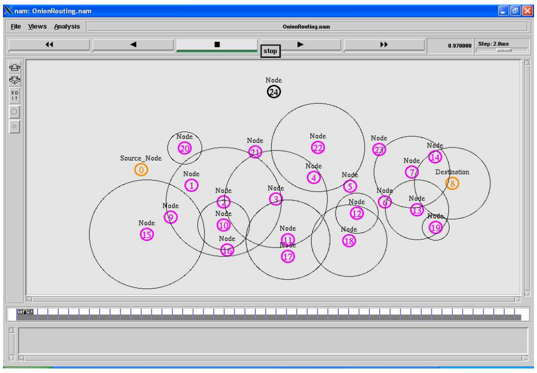

Fig 4 selected path in which data is going to travel from source to dest.

## VIII. Conclusion and Future Work

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. In our future work, we will improve ESTAR to reduce the packet delay. A possible method is to combine it with a trust based routing. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks.

## 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.

## BIOGRAPHY

**Ashwini** is a final year student of Rrase college of engineering in the department of computer science of engineering who is interested in networks she wants to know more and get more advanced functioning of networks .This field would teach more and more ethic detailed knowledge of networks and advanced features in it.