Securing Heterogeneous Multi-hop Wireless Sensor Networks Using E-STAR Protocol

Dhok Divya[1], Sanap Anita[2], Shermale Rupali[3], Shrivastava Anushka[4]

[1,2,3,4]Final Year Engineering (B.E), Assistant Prof. R. N. Muneshwar
Information Technology Engineering,
Amrutvahini College of Engineering, Sangamner.

---***---

Abstract - To communicate from source to destination, the multi-hop wireless networks need two or more hops. Whenever a node is located at a remote place the nodes are inter-dependent to relay the data packets. In heterogeneous multi-hop wireless networks the nodes have greatly varying requirements of hardware, energy or their mobility. In heterogeneous networks the nodes that lack in energy can break the routes as they do not have sufficient energy to relay the data packets to the destination. Due to uncertain behavior of the nodes the trustworthiness of nodes and reliability of networks reduces. In case of broken routes the nodes depend on time-out cycles for re-connecting to the routes. This can lead to network flooding and increases the latency of delivering the packets. Thus the proposed E-STAR combines trust and payment systems with the energy-aware routing protocol. The trusted party keeps account of the trust values and credits of nodes. All the above innovations are to accomplish the stability of the nodes by focusing on trusted nodes.

***Key Words*: Securing heterogeneous multi-hop wireless networks, packet dropping and selfishness attacks, trust systems, and secure routing protocols**

1. INTRODUCTION

In the project, we propose a secure protocol for Establishing Stable and reliable Routes in HMWNs. The proposed work combines trust system and payment systems with a trust-based and energy-aware routing protocol. To charge the nodes that send packets and reward the nodes that relay packets, the payment system uses credits for nodes. As a trusted party (TP) may not be involved in the communication sessions, an offline trusted party is required to manage the credit accounts of the nodes. The nodes contain proofs of relayed packets as receipts and submit them to TP. The payment system can encourage the selfish nodes to relay other nodes' packets to gain credits. The payment system can also evaluate the fairness of a node by rewarding the nodes that relay more packets like the nodes at the network center. However, the payment system is not adequate to ensure route stability. It can encourage the rational nodes not to break routes to gain credits, but the routes can be broken due to some other factors. These factors could be low resources, node failure, and malicious attacks. A node's trust value is defined as the degree of faith about the node's behavior. The trust values are calculated from the nodes' previous behaviors and used to predict their further behavior.

2. Literature Survey

1. ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-hop Wireless Networks.

In multi-hop wireless networks, selfish nodes do not relay other nodes' packets and make use of the trustworthy nodes to relay the packets, which has negative effect on the network performance. Incentive protocols use credits to stimulate the selfish nodes' cooperation, but the existing protocols usually rely on the heavy-weight public-key operations to secure the payment. In this project, we propose secure cooperation incentive protocol that uses the public-key operations only for the first packet in a series and uses the light-weight hashing operations in the further packets, such that the overhead of the packet series converges for the hashing operations. Hash chains and keyed hash results are used for achieving payment non-repudiation and prevent free riding attacks. Security analysis and performance evaluation reveal that the put forth protocol is secure and the overhead cannot be compared to the public-key based incentive protocols because the efficient hashing operations dominate the nodes' operations. Moreover, the average packet overhead is less than the asymmetric key based protocols with actually high probability due to shortening the keyed hash results.

2. An Efficient Anonymous Communication Protocol for Wireless Sensor Networks.

Anonymous communication is very important for a lot of wireless sensor networks as it can be used to conceal the identity of important nodes, such as the base station and the source node. In sensor networks the nameless communication consists several important features, such as source uncertainty, communication - relationship uncertainty, and base station uncertainty. Existing sensor network uncertain schemes not only achieve all the uncertainties, but also have large calculation, storage and communicative overheads. In this project, we propose an efficient anonymous communication protocol for sensor networks, which can achieve all the anonymities, while having small overheads on calculation, storage and communication.

3. An Acknowledgement based approach for routing misbehavior detection in MANET with AOMDV .

A Mobile Ad Hoc Network (MANET) is a collection of mobile host nodes which communicate with one another through wireless links either in a direct way or in a indirect way depending on other nodes. As the nodes in MANETs are free to move randomly, network structure of a MANETs can change in an predictable and rapid manner. Due to the dynamic change in structure finding route is very difficult. In MANETs performing network function consumes energy and other resources thus some nodes can misbehave. To detect the routing misbehavior in MANETs many techniques such as watchdog, path rater, TWOACK, SACK, End to End ACK scheme are available. But owing to the drawbacks of the above scheme a new scheme called 2 ACK is used. For path initiation, and routing an on-demand, multiple path DVSR protocol (AOMDV)is used. On demand routing protocol with multipath capability can effectively deal with mobility induced route failures in MANETs. The main motive of the 2ACK scheme is for sending acknowledgment in two hops in the direction opposite to routing path. In 2ACK scheme, to cut down the extra overhead of routing only little number of the received data packets are acknowledged.

4. Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks.

Mobile ad hoc networking has become an active research area from several years. How to set-up co-ordination among selfish mobile nodes, however, is not well addressed yet. In this project, we propose Sprite, a simple, cheat-proof, credit-based system for stimulating co-ordination within selfish nodes in mobile ad hoc networks. Our system provides incentive for mobile nodes to cooperate and be loyal to submit reports. In comparison to past approaches, our system does not require any tamper- proof hardware at any node. Further, we present an official model of our system and prove its properties. Evaluations of a implemented prototype show that the overhead of our system is small.

5. PIS: A Practical Incentive System for Multi-hop Wireless Networks

In multi-hop wireless networks (MWNs), the mobile nodes usually act as routers to relay other nodes' packets to enable new applications and enhance network performance and deployment. However, selfish nodes may not cooperate and make use of the cooperative nodes to relay their packets, which has a negative effect on network fairness, security, and performance. Incentive systems implement micropayment in the network to stimulate the selfish nodes to cooperate. However, micropayment schemes have originally been proposed for Web-based applications; therefore, a practical incentive system should consider the differences between Web-based applications and cooperation stimulation. In this project, first, these differences are investigated, and a payment model is developed for the efficient implementation of micropayment in MWNs. Second, based on the developed payment model, an incentive system is proposed to stimulate the nodes' cooperation in MWNs. Third, a reactive receipt submission mechanism is proposed to reduce the number of submitted receipts and protect against collusion attacks. Extensive analysis and simulations demonstrate that our incentive system can secure the payment and reduce the overhead of storing, submitting, and processing payment receipts significantly, which can improve the system's practicality due to the high frequency of low-value payment transactions.

3. Architecture

We describe the architecture of our proposed system.

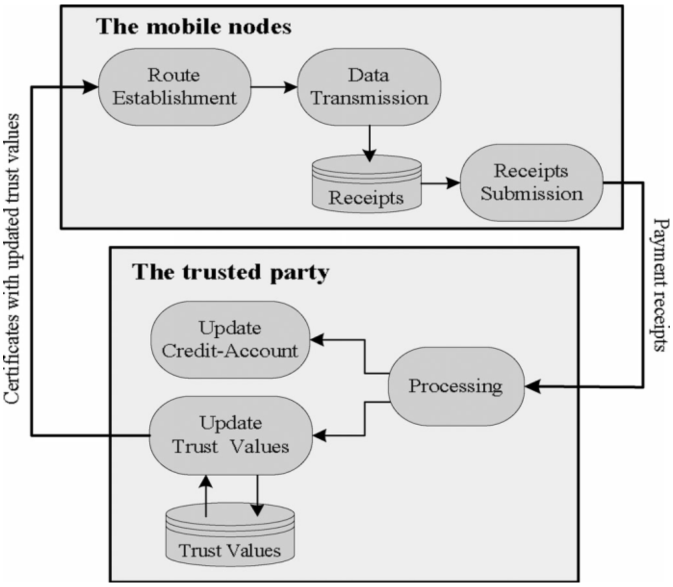

Figure 3.1: Proposed System.

3.1 System description

The proposed E-STAR operates in three main phases:
1. The Data Transmission phase.
2. Update Credit Accounts and Trust Values phase.
3. The Route Establishment phase.

1. The Data Transmission Phase

We have considered the node 'Ns' to be the source node and the node 'Nd' to be the destination node. 'Ns' wants to send data to the node 'Nd' with the nodes 'Nx', 'Ny', 'Nz' being intermediate between them. This route is established by the routing protocols SRR and BAR. For say 'i'th data packet, 'Ns' calculates the signature ἐs(i) = {H(H(mi),ts,R,i)}Ks+ and sends the packet “<R,ts,I,mi, ἐs(i) >” to the first node in the route. R, ts and mi are the concatenation of the nodes in the route (R = IDs, IDx, IDy, IDz, IDd), the route establishment time stamp, and the ‘i’th message respectively.

2. Update Credit Accounts and Trust Values phase.

When TP receives a receipt, it first checks if the receipt has been processed before using its unique identifier (R, ts). The signatures of the nodes are verified by the TP and then the signatures are hashed. The receipt is valid if the resultant hash value is identical to the receipt’s cryptographic token. TP verifies the destination node’s hash chain by making sure that hashing ‘hi’ ‘i’ times produces ‘h0’. TP clears the receipt by rewarding the intermediate nodes and debiting the source and destination nodes. The number of sent messages (iÞ is signed by the source node and the number of delivered messages can be computed from the number of hashing operations to obtain ‘h0’ from ‘hi’.

3. The Route Establishment phase.

We present two routing protocols called the shortest reliable route and the best available route. SRR establishes the shortest route that can satisfy the source node’s trust, energy, and route-length requirements, but the destination node selects the best route in the BAR protocol.
The routing protocols have three processes:
1) Route request packet (RREQ) delivery.
2) Route selection.
3) Route reply packet (RREP) delivery.

CONCLUSION:

By analyzing the nodes behavior E-STAR makes all the routing decisions and this is done by considering many factors that include the route length, the reliability of the node and its lifetime. We have made use of two important protocols for the implementation. The Shortest Reliable Route (SRR) protocol chooses a route such that the energy requirements of the nodes are fulfilled. It is useful in establishing routes that avoid the low-trust nodes. The Best Available Route (BAR) protocol allows the destination nodes to set up routes that are most reliable. However the BAR protocol involves more overhead than SRR protocol. According to the analytical outcomes, E-STAR does not imply false accusations and secures the payment and trust calculations. Besides, the simulation results prove the improved and efficient Packet Delivery Ratio (PDR) as it stabilizes the routes.

REFERENCES

[1] Secure and Reliable Routing Protocols for Heterogeneous Multi-hop Wireless Networks. IEEE Transactions on Parallel And Distributed Systems, Vol. 26, No. 4, April 2015.

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

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

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

[5] sAn 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.