INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

TRUST AND SECURE BASED SCHEME FOR MULTI-HOP WIRELESS NETWORKS USING SHORTEST RELIABLE ROUTE

Sathish Kumar.M [1]

[1] *PG SCHOLAR, M.E Computer Science and Engineering,SVS College Of Engineering, Coimbatore.*
eversathish@gmail.com
Address:7/19,Eswaran Kovil Street, T.Kottampatti,Mahalingapuram,Pollachi-642002
Mobile:+91- 7708734870
Email ID: eversathish@gmail.com

Abstract

The propose system is based on trust for establishing stable and reliable routes in heterogeneous multi-hop wireless networks. It combines payment and trust systems with a trust-based routing protocol. The payment system rewards the nodes that relay other's packets and charges those that send packets. The trust system evaluates the node's competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the node's public-key certificates to be used in making routing decisions. The routing protocols to direct traffic through those highly-trusted nodes and also nodes having sufficient energy to minimize the probability of breaking the route. By this way, it 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. Simulation results demonstrate that this routing protocol can improve the packet delivery ratio and route stability. Moreover, for the efficient implementation of the trust system, TP computes the trust values by processing the payment receipts. It uses Trust-based scheme called Shortest Reliable Route (SRR). The goal is to establish stable routes to reduce the probability of breaking routes due to the following reasons: **Lack of energy**: an intermediate node may not have sufficient energy to relay the source node's packets and keep the route connected and **node behaviour**: the nodes may break routes due to malicious action, malfunction, low hardware resources etc. SRR protocol establishes the shortest route that can satisfy the source node's requirements including energy, trust, and route length.
.

Keywords: Heterogeneous Multi-Hop, Shortest Reliable Route, Trust Values, Routing Decisions

1. Introduction

Multi-hop wireless networks use two or more wireless hops to convey information from a source to a destination. There are two distinct applications of multi-hop communication, with common features, but different applications. A wireless network adopting multi-hop wireless technology without deployment of wired backhaul links. A mobile ad-hoc network consists of a group of mobile nodes that communicate without requiring a fixed wireless infrastructure. Mobile ad hoc networks have several practical applications including battlefield communication, emergency first response, and public safety systems. 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 [1].In contrast to conventional cellular systems, there is no master-slave relationship between nodes such as Ò base station to mobile users Ó in ad-hoc networks. Communication between nodes is performed by direct connection or through multiple hop relays.

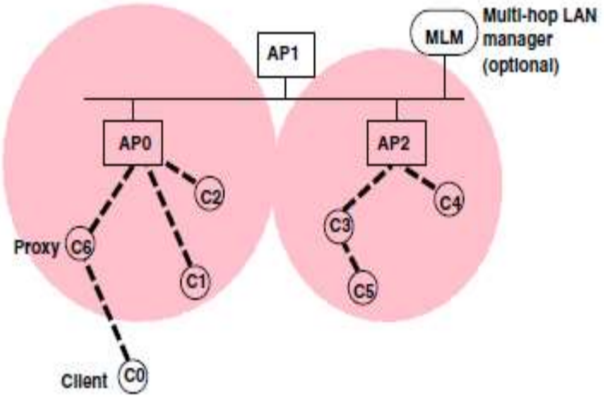


Figure No.1 Architecture of Multi-hop Wireless Network

Cellular systems conventionally employ single hops between mobile units and the base station. IEEE 802.11 based wireless LANs (WLANs) are one of the primary enablers to access the Internet. Because of this uncertainty in the node's behaviour, randomly selecting the intermediate nodes will degrade the route's stability. It will also endanger the reliability of data transmission and degrade the network performance in terms of packet delivery ratio [3]. The selfish behaviour also degrades the network connectivity significantly which may cause the Multi-hop communication to fail [4]. An obvious advantage of such architecture is the increase in the wireless coverage area. Multi-hop cellular network combine the benefits of having a fixed infrastructure of base stations and the flexibility of ad-hoc networks. They are capable of achieving much higher throughput than current cellular systems, which can be classified as Single hop Cellular Networks (SCNs) such as temperature, sound, pressure and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. In Sprite [8], each individual message the source node copies and store the signature identity of the nodes in the route and also its the message. Each intermediate node verifies the signature and submits a signed receipt to Trusted Party to claim the payment. Credits are updated in credit-update phase for each intermediate node that forwarded the message. However, the receipts overload the network because one receipt is composed for each individual message. To reduce the receipt's count, PIS [9] generates a constant size receipt per route regardless of the number of messages it generates. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications such as industrial process monitoring and control, machine health monitoring, and so on.

1.1 Applications of Multi-hop Wireless Network

- Transportation systems.
- Building automations.
- Health and medical systems.
- Security surveillance systems.
- Spontaneous networking.

1.2 Objective of the Project

The payment schemes alone are not sufficient for establishing stable routes that require selecting the nodes that behaved well in the past and have sufficient energy. The main goal is to enable the nodes to indirectly build trust relationships using exclusively monitored information. Trust values are used to decide which nodes to select/avoid in routing. Since a trust value depicts the probability that the node conducts an action, route reliability can be computed using its node trust values to give probabilistic information about the route stability and lifetime. This information is very useful for establishing stable routes and selecting proper routes that can satisfy the source node's requirements. To enhance the network performance in multi-hop wireless networks the traffic originated from a node is usually relayed through the other nodes to the destination for enabling new applications. Multi-hop packet relay can extend the network coverage using limited transmit power, improve area spectral efficiency and enhance the network throughput and capacity. Once a node's trust values fall behind those of the majority of the other nodes the node almost will not participate in routing without the need for determining good thresholds.

2. Problem Description

2.1 Existing System

A Report-based payment scheme for MWNs. The nodes submit lightweight payment reports to the AC to update their credit accounts, and temporarily store undeniable security tokens called Evidences. The reports contain the alleged charges and rewards of different sessions without security proofs, e.g., signatures. The AC verifies the payment by investigating the consistency of the reports and clears the payment of the fair reports with almost no cryptographic operations. For cheating reports the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports. RACE can identify the cheating nodes with submitting and processing few Evidences. Evidence are submitted and the AC applies cryptographic operations to verify them only in case of cheating, but the nodes always submit security tokens and the AC always applies cryptographic operations to verify the payment in the existing receipt-based schemes. Moreover, the Evidence aggregation technique is used to reduce the storage area of the Evidences.

The Evidence contains two main parts called DATA and PROOF. The DATA part describes the payment, i.e., who pays whom and how much and contains the necessary data to regenerate the node's signatures. The PROOF is an undeniable security token that can prove the correctness of the DATA and protect against payment manipulation, forgery, and repudiation. The PROOF is composed by hashing the destination node's signature and the last signature received from the source node, instead of attaching the signatures to reduce the evidence size. RACE has four main phases: Communication phase, Classifier phase, Identifying Cheaters, Credit-Account Update phase.

Some Disadvantages are

- High-mobility.
- Less trust.

2.2 Proposed System

The proposed system develops a trust system based on processing the payment reports to maintain a trust value for each node. The nodes that relay messages more successfully will have higher trust values. The payment system uses credits to charge the nodes that send packets and reward those relaying packets. It can also enforce fairness by rewarding the nodes that relay more packets such as those at the network center. Since a trusted party may not be involved in the communication sessions, an offline trusted party (TP) is required to manage the node's credit accounts. The nodes compose proofs of relaying packets, called receipts, and submit them to TP. However, the payment system is not sufficient to ensure route stability these routes can be broken due to other reasons. Multi-dimensional trust values can better predict the node's future behaviour, and thus help make smarter routing decisions. In trust system the nodes that frequently drop packets, break routes, or are not active in relaying others packets have low trust values. A node's trust values are attached to its public- key certificate to be used in making routing decisions. Trust values are used to decide which nodes to select/avoid in routing. The main benefits of integrating the payment and trust systems are First, it fosters trust among the nodes by making knowledge about the nodes past behaviour available. Second, this integration can deliver messages through reliable routes and allow the source nodes to prescribe their required level of trust. Third, it can avoid the nodes that break routes by giving more preference to the highly-trusted nodes in route selection, and thus in earning credits. Fourth, the integration of the payment and trust systems with the routing protocol can avoid the nodes that report incorrect energy capability.

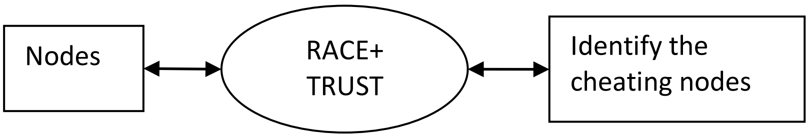
Some Advantages are

- Compare with Existing system, the proposed system is secure.
- The nodes that relay messages more successfully will have higher trust values, such as the low-mobility and the large-hardware-resources nodes.
- Highly trusted Model.

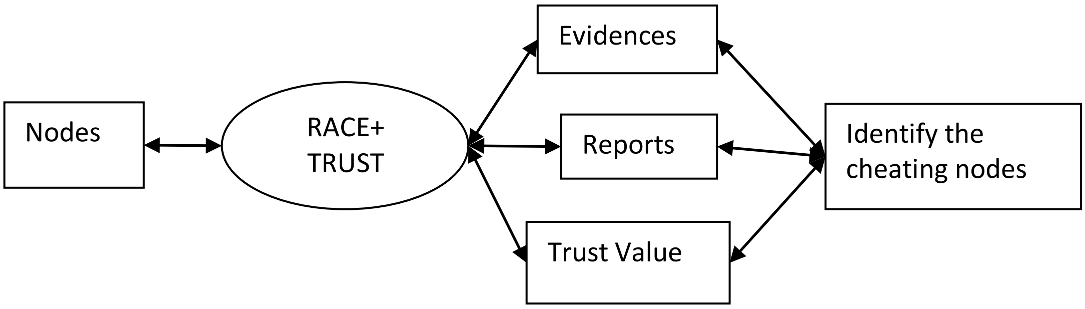
2.3 System Model

Block diagram

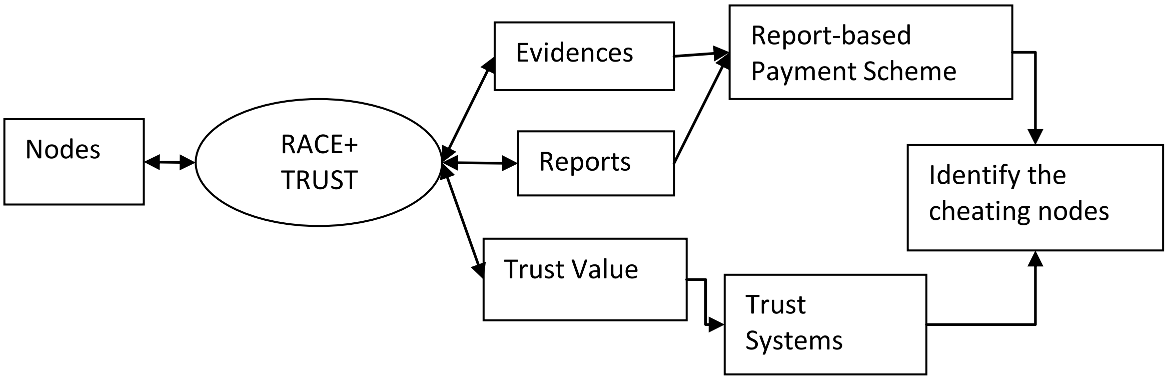
LEVEL 0



LEVEL 1



LEVEL



A network is simulated, with minimum of 30 nodes moving in a defined area. Each node moves randomly in this area, with a speed selected in a range [0, V_{max}] with no pause time. Required number of nodes are created using ns2.

2.4 Calculation of Trust Value

In this trust system that maintains multi-dimensional trusts values for each node to evaluate the node's behaviour from different perspectives. Multi-dimensional trust values can better predict the node's future behaviour, and thus help make smarter routing decisions. Here the nodes that frequently drop packets, break routes, or are not active in relaying packets have low trust values. Moreover, for the efficient implementation of the trust system, TP computes the trust values by processing the payment receipts. A node's trust values are attached to its public- key certificate to be used in making routing decisions.

Trust values are used to decide which nodes to select/avoid in routing. Since a trust value depicts the probability that the node conducts an action, route reliability can be computed using its node's trust values to give probabilistic information about the route stability and lifetime. This information is very useful for establishing stable routes and selecting proper routes that can satisfy the source node's requirements. Trust values are calculated as follows,

$$\mathrm{TP} \rightarrow \mathcal{N}_K\!: \mathrm{Cert}_K = \mathrm{ID}_K, t_e, t_j, t_i, K_{K-}, \tau_K, \{H(\mathrm{ID}_K, t_e, t_j, t_i, K_{K-}, \tau_K)\}K_{TP+}$$

$$\tau_k^{(1)} = \frac{\text{No of packets that are relayed in the last } \omega \text{ sessions}}{\text{Total No of incoming packets in the last } \omega \text{ sessions}} \quad (1)$$

$$\tau_k^{(2)} = 1 - \frac{\text{No of sessions broken by } \mathcal{N}_K \text{ in the last } \omega \text{ sessions}}{\omega} \quad (2)$$

$$\tau_k^{(3)} = \frac{\text{No of sessions that } \mathcal{N}_K \text{ relayed at least } \delta \text{ packets}}{\omega} \quad (3)$$

$$\tau_k^{(4)} = \frac{\text{No of sessions } \mathcal{N}_K \text{ paricipated in the period t}}{\mathcal{M}} \quad (4)$$

$$\tau_{WXYZ}^{(i)} = \tau_W^{(i)} \times \tau_X^{(i)} \times \tau_Y^{(i)} \times \tau_Z^{(i)} \quad (5)$$

3. Conclusion

The main idea behind this system is to calculate trust value for each available nodes and select nodes that have higher trust values based on their past history such as nodes that relay other nodes packet, nodes that do not act selfish, etc and the nodes that frequently drop packets, break routes, or are not active in relaying packets have lower trust values, are all taken into count for consideration. After all these procedure are over there exists highly trusted node based on the availability of nodes the most trusted path is calculated using the TP Formula mentioned above. Based on the most trusted path available data are transmitted using SRR. Here trust system maintains multi-dimensional trust values for each node to evaluate the node's behaviour from different perspectives. A node's trust values are attached to its public- key certificate and these trust values can better predict the node's future behaviour, and thus help in making smarter routing decisions. Moreover, for the efficient implementation of the trust system, TP computes the trust values by processing the payment receipts.

References

1) M. Mahmoud and X. Shen, "FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012.

2) M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997- 1010, July 2011.

3) M. Mahmoud and X. Shen, "PIS: A Practical Incentive System for Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

4) M. Mahmoud and X. Shen, "Stimulating Cooperation in Multi-hop Wireless Networks Using Cheating Detection System," Proc. IEEE INFOCOM '10, Mar. 2010.

5) 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.

6) H. Gharavi, "Multichannel Mobile Ad Hoc Links for Multimedia Communications," Proc. IEEE, vol. 96, no. 1, pp. 77-96, Jan. 2008.

7) B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless Network Security, Springer Network Theory and Applications, vol. 17, pp 103- 135, 2007.

8) Y. Zhang and Y. Fang, "A Secure Authentication and Billing Architecture for Wireless Mesh Networks," ACM Wireless Networks, vol. 13, no. 5, pp. 663-678, Oct. 2007.

9) J. Pan, L. Cai, X. Shen, and J. Mark, "Identity-Based Secure Collaboration in Wireless Ad Hoc Networks," Computer Networks, vol. 51, no. 3, pp. 853-865, 2007.

10) 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, pp. 192-203, Jan. 2007.

11) G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation Enforcement Schemes for MANETs: A Survey," Wiley's J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332, 2006.

12) N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "Node Cooperation in Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 4, pp. 365-376, Apr. 2006.

13) A. Weyland, T. Staub, and T. Braun, "Comparison of Motivation-Based Cooperation Mechanisms for Hybrid Wireless Networks," J. Computer Comm., vol. 29, pp. 2661-2670, 2006.

14) A. Weyland, "Cooperation and Accounting in Multi-Hop Cellular Networks," PhD thesis, Univ. of Bern, Nov. 2005.

15) O. Nibouche, M. Nibouche, A. Bouridane, and A. Belatreche, "Fast Architectures for FPGA-Based Implementation of RSA Encryption Algorithm," Proc. IEEE Field-Programmable Technology Conf., Dec. 2004.

A Brief Author Biography

Sathish Kumar.M :- Completed B.E (COMPUTER SCIENCE AND ENGINEERING) in P.A College of Engineering and Technology from Anna University, Chennai. Now Pursuing M.E (COMPUTER SCIENCE AND ENGINEERING) in SVS College of Engineering and Technology from Anna University, Chennai. My research area interests include Networks.