RESEARCH ARTICLE OPEN ACCESS

Efficiency Report Based Payment scheme for Multihop Wireless Networks

Usikela Naresh1, Roopavath Jethya2
Department of Computer Science and Engineering, AAR Mahaveer Engineering College,Hyderabad, Telangana – 500005, India
Corresponding Author: Usikela Naresh

ABSTRACT: A report-based payment scheme for multihop wireless networks to stimulate node cooperation, regulate packet transmission, and enforce fairness. The nodes submit lightweight payment reports (instead of receipts) to the accounting center and temporarily store undeniable security tokens called Evidences. The reports contain the alleged charges and rewards without security proofs, e.g., signatures. The account can verify the payment by investigating the consistency of the reports, and clear the payment of the fair reports with almost no processing overhead or cryptographic operations. For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports. Instead of requesting the Evidences from all the nodes participating in the cheating reports, report-based payment scheme can identify the cheating nodes with requesting few Evidences. Moreover, Evidence aggregation technique is used to reduce the Evidences' storage area. Our analytical and simulation results demonstrate that report based payment scheme requires much less communication and processing overhead than the existing receipt-based schemes with acceptable payment clearance delay and storage area. This is essential for the effective implementation of a payment scheme because it uses micropayment and the overhead cost should be much less than the payment value. Moreover, RACE(report-based payment scheme) can secure the payment and precisely identify the cheating nodes without false accusations**.**

Index Terms— Cooperation incentive schemes, Network Level Security and high protection, Payment Schemes, Selfishness Attacks.

Date Of Submission: 26-04-2019 Date Of Acceptance: 06-05-2019

I. INTRODUCTION

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology [1]. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may, but need not, connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. The animation below illustrates how wireless mesh networks can self form and self heal. Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type.

Wireless mesh architecture is a first step towards providing cost effective and dynamic high-bandwidth networks over a specific coverage area. Wireless mesh architectures infrastructure is, in effect, a router network minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops. Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network, i.e. perform routing. Such architecture may with careful design provide high bandwidth, spectral efficiency, and economic advantage over the coverage area.

Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The path of traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic in an infrastructure mesh network is either forwarded to or from a gateway, while in ad hoc networks or client mesh networks the traffic flows between arbitrary pairs of nodes.

Management

This type of infrastructure can be decentralized (with no central server) or centrally managed (with a central server), both are relatively inexpensive, and very reliable and resilient, as each node needs only transmit as far as the next node. Nodes act as routers to transmit data from nearby nodes to peers that are too far away to reach in a single hop, resulting in a network that can span larger distances. The topology of a mesh network is also reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbors can quickly find another route using a routing protocol.

Applications

Mesh networks may involve either fixed devices. The solutions are as diverse as communication needs, for example in difficult environments such as emergency situations, tunnels, oil rigs, battlefield surveillance, high speed video applications on board public transport or real time racing car telemetry. An important possible application for wireless mesh networks is VoIP. By using a Quality of Service scheme, the wireless mesh may support local telephone calls to be routed through the mesh.

Some current applications:

- U.S. military forces are now using wireless mesh networking to connect their computers, mainly ruggedized laptops, in field operations.
- Electric meters now being deployed on residences transfer their readings from one to another and eventually to the central office for billing without the need for human meter readers or the need to connect the meters with cables.
- The laptops in the One Laptop per Child program use wireless mesh networking to enable students to exchange files and get on the Internet even though they lack wired or cell phone or other physical connections in their area.
- The 66-satellite Iridium constellation operates as a mesh network, with wireless links between adjacent satellites. Calls between two satellite phones are routed through the mesh, from one satellite to another across the constellation, without having to go through an earth station. This makes for a smaller travel distance for the signal, reducing latency, and also allows for the constellation to operate with far fewer earth stations that would be required for 66 traditional communications satellites.

Operation

The principle is similar to the way packets travel around the wired Internet— data will hop from one device to another until it reaches its destination. Dynamic routing algorithms implemented in each device allow this to happen. To implement such dynamic routing protocols, each device needs to communicate routing information to other devices in the network. Each device then determines what to do with the data it receives — either pass it on to the next device or keep it, depending on the protocol. The routing algorithm used should attempt to always ensure that the data takes the most appropriate (fastest) route to its destination.

Multi-radio mesh

Multi-radio mesh refers to a unique pair of dedicated radios on each end of the link. This means there is a unique frequency used for each wireless hop and thus a dedicated CSMA collision domain. This is a true mesh link where you can achieve maximum performance without bandwidth degradation in the mesh and without adding latency. Thus voice and video applications work just as they would on a wired Ethernet network. In true 802.11 networks, there is no concept of a mesh. There are only Access Points (AP's) and Stations. A multi-radio wireless mesh node will dedicate one of the radios to act as a station, and connect to a neighbor node AP radio.

The existing payment schemes can be classified into tamper-proof-device(TPD)-based and receipt-based schemes[2][3]. In TPD-based payment schemes, a TPD is installed in each node to store and manage its credit account and secure its operation. For receipt-based payment schemes [4][5][6][7][8][9] an offline central unit called the accounting center stores and manages the nodes' credit accounts. The nodes usually submit undeniable proofs for relaying packets, called receipts, to the AC to update their credit accounts.

Disadvantages:

- False accusations and missed detections
- Vulnerable to Collusion attacks
- Long time to identify cheaters

Algorithm 1: Data transmission/composition of *Evidence* and report

```
1: // n_i is the source, intermediate, or destination node that is running the algorithm.
2: if (n_i is the source node) then
3:       P_X ←[R, X, Ts, M_X, Sig_S(R, X, Ts, H(M_X ))];
4:       Send(P_X);                    // send P_X to the first node in the route
5: else
6:       if ((R, X, Ts are correct) and Verify(Sig_S(R, X, Ts, H(M_X))) == TRUE) then
7:             if (n_i is an intermediate node) then
8:                Relay the packet;
9:                Store Sig_S(R, X, Ts, H(M_X));
10:            end if
11:            if (n_i is the destination node) then
12:               Send(h^(X));
13:            end if
14:      else
15:            Drop the packet;
16:            Send error packet to the source node;
17:      end if
18: end if
19: if (P_X is last packet) then
20:      Evidence = {R, X, Ts, H(M_X), h^(0), h^(X), H(Sig_S(R, X, Ts, H(M_X))), Sig_D(R, Ts, h^(0))};
21:      Report = {R, Ts, F, X};
22:      Store Report and Evidence;
23: end if
```

System Modules:
1. Data Transmission
2. Evidence Composition
3. Payment Report Composition/Submission

1. Data Transmission

The source node sends data packets to the destination node through the established route and the destination node replies with ACK packets. For the Xth data packet, the source node appends the message MX and its signature to R, X, Ts (Algorithm 1), and the hash value of the message and sends the packet to the first node in the route. The security tokens of the Xth data and ACK packets are illustrated. The source node's signature is an undeniable proof for transmitting X messages and ensures the message's authenticity and integrity.

2. Evidence Composition

Evidence is defined as information that is used to establish proof about the occurrence of an event or action, the time of occurrence, the parties involved in the event, and the outcome of the event. Fig 1The purpose of Evidence is to resolve a dispute about the amount of the payment resulted from data transmission.

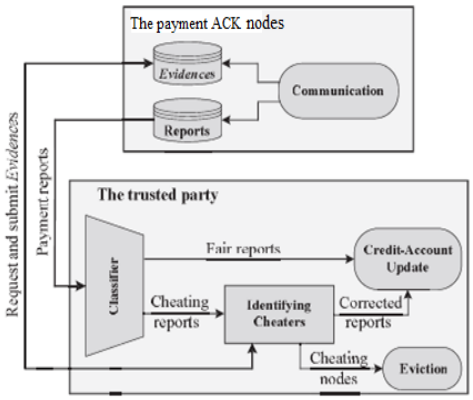

Fig : 1. The Architecture of RACE

3. Payment Report composition/ Submission

A payment report is updated by the Trusted Party. After the Trusted Party verification any transaction is updated. By using the Certificate, Public Key, Symmetric Key, the transaction is approved. If the transaction is faulty or fraud, then the Trusted Party verifies it and the transaction is cancelled. The transaction amount will not be updated in the receiver account.

we propose RACE, a Report-based payment scheme for WMNs(Wireless Mesh Networks). The nodes submit lightweight payment reports (instead of receipts) to the AC (Account) 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 or computational overhead. For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports, e.g., to steal credits or pay less. In other words, the Evidences are used to resolve disputes when the nodes disagree about the payment. Instead of requesting the Evidences from all the nodes participating in the cheating reports, RACE (fig 1) can identify the cheating nodes with submitting and processing few Evidences. Moreover, Evidence aggregation technique is used to reduce the storage area of the Evidences.

In RACE, Evidences are submitted and the AC applies cryptographic operations to verify them only in case of cheating, but the nodes always submit security tokens, e.g., signatures, and the AC always applies cryptographic operations to verify the payment in the existing receipt based schemes. RACE can clear the payment nearly without applying cryptographic operations and with submitting lightweight reports when Evidences are not frequently requested.

Advantages:

Widespread cheating actions are not expected in civilian applications because the common users do not have the technical knowledge to tamper with their devices. Moreover, cheating nodes are evicted once they commit one cheating action and it is neither easy nor cheap to change identities. Our analytical and simulation results demonstrate that RACE requires much less communication and processing overhead than the existing receipt-based schemes [4] with acceptable payment clearance delay and Evidences' storage area, which is necessary to make the practical implementation of the payment scheme effective.

Comparison between RACE and the Existing Payment Schemes

	RACE	Receipt-based schemes [11-13, 17]	CDS
Communication overhead	Low	Large	Low
Payment processing overhead	Fair reports: light overhead Cheating reports: Cryptographic operations are applied	Cryptographic operations are systematically applied	Lightweight statistical operations
Payment clearance delay	Much shorter than CDS in case of cheating	The shortest delay	Very long delay in case of cheating
Storage area	More than receipt-based schemes	More than CDS and less than RACE	Smallest storage area
Security	- No false accusations and missed detections - Strong protection against colluders - Cheaters are identified after the first cheating action	- No false accusations and missed detections - Strong protection against colluders - Cheaters are identified after the first cheating action	- False accusations and missed detections. - Vulnerable to collusion attacks - Long time to identify cheaters

Fig**: 2** RACE and EPS (Existing Payment Scheme)

Moreover, RACE can secure the payment and precisely identify the cheating nodes without false accusations or stealing credits. To the best of our knowledge, RACE (fig 2) is the first payment scheme that can verify the payment by investigating the consistency of the nodes' reports without systematically submitting and processing security tokens and without false accusations. RACE is also the first scheme that uses the concept of Evidence to secure the payment and requires applying cryptographic operations in clearing the payment only in case of cheating.

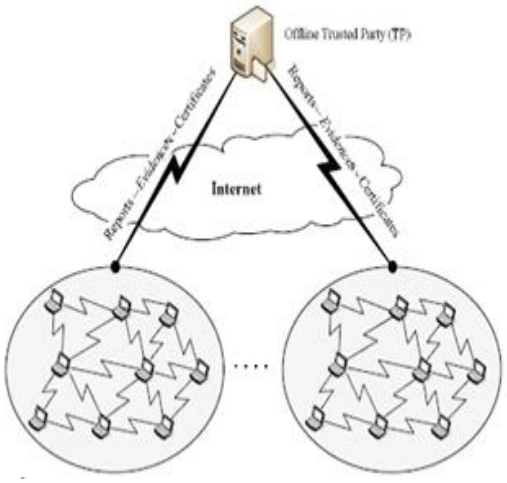

Fig: 3. The Architecture of considered Network

The above architecture it shows how to transfer funds one node to other node. Fig: 3 Here before transferring fund users must register with particular details. After registration Symmetric key and public key it will generate for secure transfer funds. Then users login with their user ids for making transfer fund between two user but the receiver must be in receiver mode.

We have to assign ip address of destination while submitting the request, if it is reach to particular destination then it will start the transaction. After completion of the transaction then trusted party verify it for verification. If trusted party verifies the transaction by using the key and then only the transaction will be updated. If any fault transaction occurs then the trusted party verifies and the account will not be updated with that fraud or fault transaction.

A Secure Authentication and Billing Architecture for Wireless Mesh Networks

Wireless mesh networks (WMNs) are gaining growing interest as a promising technology for ubiquitous high-speed network access. While much effort has been made to address issues at physical, data link, and network layers, little attention has been paid to the security aspect central to the realistic deployment of WMNs. We propose UPASS, the first known secure authentication and billing architecture for large-scale WMNs. UPASS features a novel user-broker-operator trust model built upon the conventional certificate-based cryptography and the emerging ID-based cryptography. Based on the trust model, each user is furnished with a universal pass whereby to realize seamless roaming across WMN domains and get ubiquitous network access. In UPASS, the incontestable billing of users is fulfilled through a lightweight real-time micropayment protocol built on the combination of digital signature and one-way hash-chain techniques. Compared to conventional solutions relying on a home-foreign-domain concept, UPASS eliminates the need for establishing bilateral roaming agreements and having real-time interactions between potentially numerous WMN operators. Our UPASS is shown to be secure and lightweight, and thus can be a practical and effective solution for future large-scale WMNs.

II. CONCLUSION:

A report-based payment scheme for MWNs. The nodes submit lightweight payment reports containing the alleged charges and rewards (without proofs), and temporarily store undeniable security tokens called Evidences. The fair reports can be cleared with almost no cryptographic operations or processing overhead, and Evidences are submitted and processed only in case of cheating reports in order to identify the cheating nodes. Our analytical and simulation results demonstrate that RACE can significantly reduce the communication and processing overhead comparing to the existing receipt-based payment schemes with acceptable payment clearance delay and Evidences' storage area, which is necessary for the effective implementation of the scheme. Moreover, RACE can secure the payment, and identify the cheating nodes precisely and rapidly without false accusations or missed detections.

Feature Work:

In RACE, the AC can process the payment reports to know the number of relayed/dropped messages by each node. In our future work, we will develop 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, such as the low-mobility and the large-hardware-resources nodes. Based on these trust values, we will propose a trust-based routing protocol to route messages through the highly trusted nodes (which performed packet relay more successfully in the past) to minimize the probability of dropping the messages, and thus improve the network performance in terms of throughput and packet delivery ratio. However, the trust system should be secure against singular and

collusive attacks, and the routing protocol should make smart decisions regarding node selection with low overhead.

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

[3]. 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.

[4]. 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.

[5]. M. Mahmoud and X. Shen, "Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System," Proc. IEEE INFOCOM '10, Mar. 2010.

[6]. 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.

[7]. M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, Oct. 2011.

[8]. H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 4628-4639, Oct. 2009.

[9]. R. Lu, X. Lin, H. Zhu, X. Shen, and B.R. Preiss, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.

Usikela Naresh " Efficiency Report Based Payment scheme for Multihop Wireless Networks" International Journal of Engineering Research and Applications (IJERA), Vol. 09, No.05, 2019, pp. 70-74