ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Cost effective Payment method for Wireless Network Enabled Devices With Less Overheads.

Thadikamala Chaitanya Krishna
M.Tech,Student ,
Computer Science Engineering Department,
Rao & Naidu Engineering College, Ongole.

N.Venkateswararao
Asst Professor & HoD,
Computer Science Engineering Department,
Rao & Naidu Engineering College, Ongole.

Abstract:

Wireless enabled devices are having increasing presence in our day to day life. Wireless Enabled is a system normally on laptops which allows you to access the Internet via an existing Internet connection. For example; If you buy a laptop which is wireless enabled, and you wish to get on to the Internet then you can do if you have a wireless router. Now days PDAs, Smart Phones, Tablets and wearable gadgets are wireless enabled. We need a secure and cost-effective payment system for this ever growing demand. In this paper, we are proposing a system, where in report based system is used instead of receipt based system.

A report is tendered by each node to a trusted party after the completion of Communication. Based on the reliability of the report the payment is done. Payment is done for the genuine reports without any processing overhead. Proper steps are in place to avoid payments for cheating nodes. These steps may vary from requesting evidences for reports to evicting the cheating nodes from the network.

Our analytical and simulation results reveal that RACE requires much less communication and processing overhead than the existing receipt-based schemes with acceptable payment clearance delay and storage area. This is vital for the effective implementation of a payment scheme for the reason that it uses micropayment and the overhead cost should be much less than the payment value. Moreover, RACE can secure the payment and accurately recognize the cheating nodes without false accusations.

Keywords:

Wirelss Networks, AD-HoC Netwrorks, Payment system, Nodes.

Introduction:

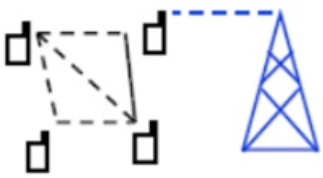
Multihop Wireless Network (MWN) is a wireless network adopting multihop wireless technology without deployment of wired backhaul links. Similar to Mobile Ad hoc Networks (MANET), but Nodes in MWN is relative 'fixed' where as in MWN may introduce 'hierarchy' network architecture.

In multi-hop wireless networks, communication between two end nodes is carried out through a number of intermediate nodes whose function is to relay information from one point to another. Multihop Wireless Netowrks are basically of two types:

1. Relay : Tree based topology, one end of the path is the base station and other end is the wireless enabled end user device. In here infrastructure is usually owned by carrier.

and

2. Mesh: Mesh topology, multiple connections exists among users. Routing by carrier owned infrastructure and/or subscriber equipment.



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Advantages of multi-hop Wireless technology:

- Rapid deployment with lower-cost backhaul.
- Easy to provide coverage in hard-to-wire areas.
- Under the right circumstances, it may
- Extend coverage due to multi-hop forwarding.
- Extend coverage due to multi-hop forwarding.
- Enhance throughput due to shorter hops.
- Extend battery life due to lower power transmission.

Disadvantages of multi-hop Wireless technology

- Routing complexity.
- Path management.
- Extra delay due to multihop relaying.

Payment Schemes:

There are various payment schemes used in various MANETs and other Ad-HoC Networks. These schemes generally selected depending on the number of nodes and who owns the infrastructure. Types of Schemes:

1.Key-based schemes.

2.The reputation-based model.

3.Credit-based model.

A selfish node, in order to save battery life, will not participate in routing and forwarding tasks, in turn affecting the overall performance of the network. Where as a malicious node, alters the data in protocol fields and divert/deny traffic to the genuine nodes. In order to motivate nodes to participate in transmitting of packets for others, they need to and incentive scheme.The nodes earn credits or points for transmitting others' packets and spend these credits/points to get their packets transmitted by others.

In addition to assist encouragement, these schemes can impose fairness, discourage Message-Flooding attacks, regulate packet transmission, and resourcefully charge for the network services. Fairness can be imposed by rewarding the nodes that transmit more packets and charging the nodes that send more packets.

For instance, the nodes located at the network center transmit more packets than the other nodes as they are more often preferred by the routing protocol.

Existing System:

The existing payment schemes can be classified into tamper-proof-device (TPD)-based and receipt-based schemes. 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, 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 Of Existing System:

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

Proposed System:

In this paper, we propose RACE, a Report-based pAyment sChemE for MWNs. The nodes submit lightweight payment reports (instead of receipts) 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 or computational overhead.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

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 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.

Report based Payment Scheme:

In a Report-based Payment Scheme for Mobile Wireless Networks, the participating nodes submit low overhead payment reports to the accounting center to update the credit accounts, and for the time being store indisputable security tokens called evidences. The reports consists the assumed charges and rewards of different sessions without any kind of verifications. The Accounting center validates the payment by examining the reliability of the reports, and clears the payment of the genuine reports with almost no overhead.

For cheating reports, the evidences are called for to recognize, report and evict the cheating nodes that submit inaccurate reports. The evidences are employed to determination of disputes when the nodes disagree about the payments done. As a substitute of requesting the evidences from all the nodes participating in the cheating reports, this system can identify the cheating nodes by processing few evidences. Evidence aggregation technique is employed to trim down the storage space of the Evidences.

Advantages Of Proposed System:

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 with acceptable payment clearance delay and Evidences' storage area, which is necessary to make the practical implementation of the payment scheme effective. 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 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.

In overall we summarize:

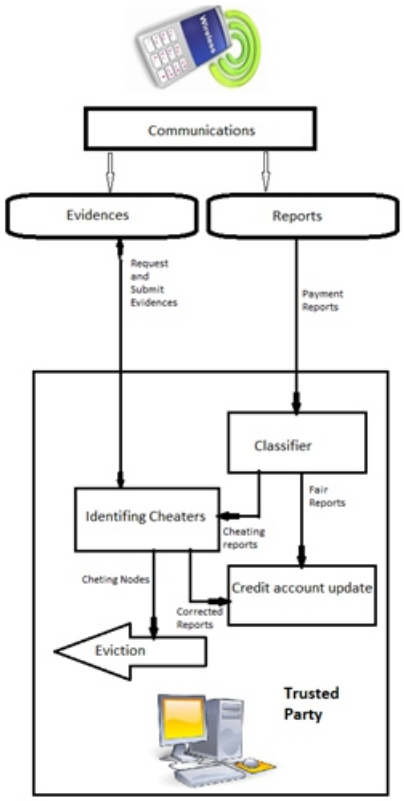
- Lightweight payment reports (charges and rewards) without security proof
- Almost no cryptographic operations in clearing payments of fair reports
- Uses Evidences to solve disputes
- Reduce storage via Evidence aggregation technique.

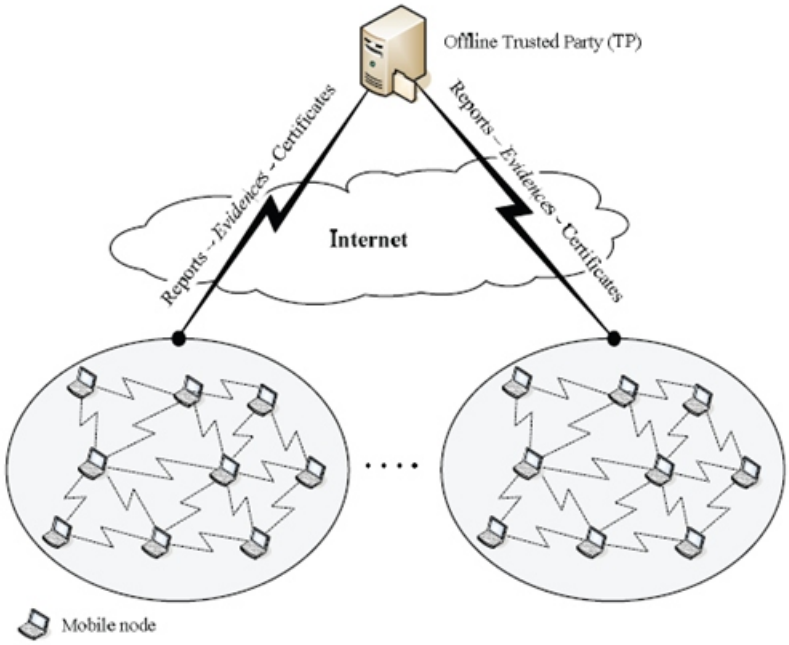
To the best of our knowledge, RACE is the first payment scheme that can verify the payment by investigating the consistency of the nodes' reports without systematically submit- ting and processing security tokens and without false accusations.

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. That the overall credits in the network decline gradually with using TPD-based schemes because the total charges may be more than the total rewards. This is because the source node is fully charged after sending a packet but some intermediate nodes may not be rewarded when the route is broken.

Architecture of Report based Payment Scheme:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal





The architecture of the considered network.

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: $P_X \leftarrow [R, X, Ts, M_X, Sig_S(R, X, Ts, H(M_X))]$;
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**

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

```
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
```

Algorithm 2: Submission/clearance of reports and Evidences

```
1: n_i → TP: Submit(Reports[t_i-1, t_i));
2: TP → n_i: Evidences_Request(Ses_IDs[t_i-2, t_i-1));
3: n_i → TP: Submit(Req_Evs[t_i-2, t_i-1));
4: TP: Identify_Cheaters();
5: TP: Clear the payment of the reports;
6: if (n_i is honest) then
7:    TP → n_i: A renewed certificate;
8: endif
```

MODULES:

1) Route establishment.

2) Data transmission.

3) Evidence composition.

4) Payment report composition/submission.

Communication Phase:

The Communication phase has four processes: route establishment, data transmission, Evidence composition, and payment report composition or submission. 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.

The purpose of an Evidence is to resolve a dispute about the amount of the payment resulted from data transmission.

Evidences have the following main features:

• Evidences are unmodifiable : If X messages are delivered, the intermediate nodes can compose Evidences for fewer than X messages, but not for more. The intermediate nodes cannot compose Evidences for more than X because it is computationally infeasible to compute .

• If the source and destination nodes collude, they can create Evidences for any number of messages because they can compute the necessary security tokens.

• Evidences are unforgeable: If the source and destination nodes collude, they can create Evidence for sessions that did not happen, but the intermediate nodes cannot, because forging the source and destination nodes' signatures is infeasible.

• Evidences are undeniable: This is necessary to enable the TP to verify them to secure the payment.

• A source node cannot deny initiating a session or the amount of payment because it signs the number of transmitted messages and the signature is included in the Evidence.

• An honest intermediate node can always compose valid Evidence even if the route is broken or the other nodes in the route collude to manipulate the payment. This is because it can verify the Evidences to avoid being fooled by the attackers.

Classifier Phase:

After getting a payment reports, the accounting Center validates them by inspecting the reliability of the reports, and categorizes them into fair or cheating. For fair reports, the nodes submit correct payment reports, but for cheating reports, at least one node does not submit the reports or submits incorrect reports to steal credits or pay less.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Identifying Cheaters:

In the Identifying Cheaters' phase, the Trusted party processes the cheating reports to identify the cheating nodes and correct the data. The main purpose is preventing the attackers from stealing credits or paying less, the attackers should not benefit by cheating.

The accounting Center requests the Evidence only from the node that submits report with more payment instead of all the nodes in the route because it should have the necessary and undeniable proofs for identifying the cheating node. In this way, the accounting Center can precisely identify the cheating nodes with requesting few Evidences.

Maintaining Trust based Protocol:

In order to decrease the overhead and to provide more security the trust based protocol is implemented. Each nodes are allocated a trust value. Depending on sending the packet effectively a trust value is allocated. The maximum trust value is allocated for the nodes that transmit packets more effectively.

Credit Account Update:

The Credit Account Update phase receives fair and corrected payment reports to update the nodes financial accounts. The accounting Center in report based Payment Scheme has to wait until receiving the reports of all nodes in a route to verify the payment.

Conclusion:

In this paper, we have observed and evaluated a report-based payment scheme for Mobile Wireless Networks. The nodes tender low overhead payment reports consisting of the proposed charges and rewards. The fair reports can be cleared with almost no overhead, and Evidences are requested, presented and processed only in case of cheating reports in order to recognize the cheating nodes.

Report based Payment Scheme can get the payment, and identify the cheating nodes accurately and quickly without any disputes, false accusations or missed detections.

In Report based Payment Scheme, the accounting Center can process the payment reports to know the number of transmitted/dropped packets by each participating node. The nodes that transmit packets more effectively will be given higher trust values.

However, the trust system should be secure against singular and collusive attacks, and the routing protocol should make intelligent decisions regarding node selection with low overhead.

References:

[1] Mahmoud And Xuemin Shen: A Secure Payment Scheme With Low Communication And Processing Overhead For Multihop wireless networks., IEEE Transactions On Parallel And Distributed Systems, Vol. 24,No. 2, pp. 209-224, February 2013.

[2] 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.

[3] 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.

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

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom00, pp. 255-265, Aug. 2000.

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

[7] 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

[8] L. Buttyan and J. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 8, no. 5, pp. 579-592, Oct. 2004.

[9] Y. Zhang, W. Lou, and Y. Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks," ACM Wireless Networks, vol. 13, no. 5, pp. 569-582, Oct. 2007.

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

[11] L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Trustful and Cost-Efficient Routing Protocol for Mobile Ad Hoc Networks with Selfish Agents," Proc. ACM MobiCom, Sept. 2003.

[12] H. Pagnia and F. Gartner, "On the Impossibility of Fair Exchange Without a Trusted Third Party," Technical Report TUD-BS-1999- 02, Darmstadt Univ. of Technology, Mar. 1999.

[13] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated Routing for Ad Hoc Networks," IEEE Selected Areas in Comm., vol. 23, no. 3, pp. 598- 610, Mar. 2005.

[14] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. ACM MobiCom, Sept. 2002.

[15] 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.

[16] S. Even, O. Goldreich, and S. Micali, "On-Line/off-line Digital Signatures," Crypto '89: Proc. Advances in Cryptology, pp. 263-277, 1990.

[17] 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.

[18] 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.

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

[20] 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.