IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. VI (Mar-Apr. 2014), PP 38-43
www.iosrjournals.org

Trust Based Secure Payment Scheme for Multi-hop Wireless Networks

Mrs. Chinchu .V. S[1] , Ms. Meji Jose[2]
[1, 2](Department of Computer Science and Engineering
Nehru College of Engineering and Research Center, Pampady, Thrissur,Kerala)

Abstract: *In this paper we propose a secure payment scheme called, trust based micro payment scheme for multihop wireless networks. This micro payment scheme enhances the cooperation of nodes and fairness of the network. Each node is assigned a trust value. Based on the trust value, a trust based routing protocol is maintained to route the packet. A report is submitted by each node to a trusted party after the communication. Based on the consistency of the report the payment is cleared. For the fair reports without any processing overhead the payment is cleared. In the case of cheater nodes more cryptographic operations and processing is required to analyze the evidences, which is submitted by each node to the trusted party ,when an inconsistent report is submitted. The report contains the alleged charges for relaying the packets. The RACE performs less cryptographic operation and processing overhead. It uses the micro payment and the overhead cost is much less than the payment value. Moreover, RACE can secure the payment and precisely identify the cheating nodes without false accusations.*

Keywords: *Payment scheme; selfish nodes; micro payment; multihop networks*

I. Introduction

In a multihop 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. Cellular systems conventionally employ single hop between mobile units and the base station. As cellular systems evolve from voice centric and data centric communication, edge-of-cell throughput is becoming a significant concern. A promising solution to the problem of improving coverage and throughput is the use of relays. Thus the multihop wireless networks evolve increasing attention and demands over the network communication. MWNs can also implement many useful applications such as data sharing and multimedia data transmission.

Selfish nodes will not relay others' packets and make use of the cooperative nodes to relay their packets, which degrades the network connectivity and fairness. The fairness issue arises when the selfish nodes make use of the cooperative nodes to relay their packets without any contribution to them, and thus the cooperative nodes are unfairly overloaded because the network traffic is concentrated through them. The selfish behavior also degrades the network connectivity significantly, which may cause the multihop communication to fail. The presents of the selfish nodes arise the need for payment scheme. Selfish nodes will not relay others' packets and make use of the cooperative nodes to relay their packets, which degrades the network connectivity and fairness. The fairness issue arises when the selfish nodes make use of the cooperative nodes to relay their packets without any contribution to them, and thus the cooperative nodes are unfairly overloaded because the network traffic is concentrated through them. The selfish behavior also degrades the network connectivity significantly, which may cause the multihop communication to fail. In order to handle the situation, the payment scheme is introduced.

In a Trust-based payment scheme for MWNs the nodes are assigned a trust value. Based on the trust value the routing is performed. Trust value is assigned based on relaying packet successfully. Each node submit light-weight payment reports to the AC to update the credit accounts, and temporarily store undeniable security tokens called evidences. The reports contain the alleged charges and rewards of different sessions without security proofs. 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. The evidences are used to resolve disputes when the nodes disagree about the payment. For the cheating nodes the cheating count is maintained to modify the trust value.

II. Related Works

The employment of adequate trust methods in mobile ad hoc networks has been receiving increasing attention during the last few years, and several trust and security establishment solutions that rely on cryptographic and hashing schemes have been proposed. These schemes, although effective, produce significant processing and communication overheads and consume energy, and, hence, they do not take into account the

idiosyncrasies of a MANET. More recently, cooperation enforcement methods have been proposed for trust establishment in MANET. These schemes, classified as reputation-based and credit-based, are considered suitable for ad hoc networks, where key or certificate distribution centers are absent or ephemerally present, and for networks that consist of devices with limited processing, battery, and memory resources. Cooperation enforcement methods do not provide strong authentication of entities. Instead, they contribute to the identification of the trustworthiness of peers and to the enforcement cooperation using mutual incentives. This paper surveys the most important cooperation enforcement methods that have been introduced, providing a comprehensive comparison between the different proposed schemes.

A MANET is a self-organized wireless network, consisting of nodes responsible for its creation, operation and maintenance. Due to mobility, the number of nodes and the topology of the network vary with time. The nodes of a MANET follow their motivation to participate as a co-operation rule, if they behave rationally. A newcomer's incentive is to offer functions such as routing and packet forwarding to the other nodes, which, in their turn, return this by offering connectivity services. Such reciprocity principles can be used to establish trust among the nodes, which is essential for the steady-state operation of a MANET. Adjacent nodes may build up trust with time, and provide this knowledge to the other nodes as a reputation. On the other hand the value of this trust diminishes when these nodes, due to their mobility, become distant. Thus, the trust established between two nodes might be lost with time, influencing network's performance. Moreover, all the nodes behave rationally, since passionate behaviors might occur. Selfish, malicious, and hacker nodes may easily follow the reciprocity principles in order to be connected on a MANET, but the intentions might be tainted. A selfish node disinclines to spend its resources for serving network's operations and maximizing the social welfare. Instead, it cooperates when the network tasks maximize its own profit. A malicious node attacks to damage network's operation, through denial of service attacks, such as sinkhole, flooding, or sleep deprivation torture, or through packet dropping and misrouting. Selfish and malicious nodes misbehave, and, intentionally or unintentionally, attack on the robustness of the MANET and produce congestions. Finally, a hacker node might try to intercept the information exchanged between the nodes. Such violation is materialized through wormhole, impersonation, or Sybil attacks. Selfish, malicious, and hacker nodes fabricate attacks against physical, link, network, and application layer functionality[3].

The current widely accepted security solution for WMNs is based on Authentication, Authorization and Accounting architecture, where the authentication request is issued by the mobile user and is sent through the serving MAP and the MGW, until reaching a centralized authentication server that can grant access to the MU. Such a long signaling path, however, could take up to one or a few seconds of propagation, and might cause fatal impairment on the emerging real-time services. Recently, many fast authentication schemes such as predictive authentication, pre-key-distributions, and enhanced inter-access point protocol, have been reported to support seamless handover when an MU roams between adjacent MAPs under a common WISP domain. On the other hand, the existing fast authentication techniques cannot be directly applied to inter-domain handoff, since it requires a bilateral service level agreement established between each pair of WISPs.

The best practice for establishing a trust relationship among different WISPs so far is by way of a centralized roaming broker trusted by all the WISPs . Under this framework, when an MU roams into a foreign network domain, the foreign WISP simply forwards the corresponding AAA session of the MU to the home WISP of the MU for authorization via the RB. A more elaborated approach can be devised on top of the centralized RB architecture by taking advantages of the public key infrastructure, where the RB serves as not only a trusted third party, but also a certificate authority, which issues public key certificates to the WISPs and MUs. The trust relationship among WISPs, or between a WISP and MUs, can be easily established by validating the public key certificates issued by the RB. In both cases, the foreign WISP reports the accounting information of the roaming MU to its home WISP at the completion of the session, by which the home WISP will pay the bill and then charge the MU in terms of the MU's spending. The RB architecture can effectively solve the interdomain roaming and billing problem, unfortunately, the RB may become a performance bottleneck for the interdomain handoff authentication and billing. In addition, the long signaling propagation latency of every transaction may not be tolerable to the real-time services in the inter-domain roaming events. Thus, the development of a new framework in meeting with the stringent requirements causes authentication latency and scalability without losing the security assurance[4].

In military and rescue applications of mobile ad hoc networks, all the nodes belong to the same authority, therefore, the motivation to cooperate in order to support the basic functions of the network. In this case when each node has its own authority and tries to maximize the benefits it gets from the network. More precisely, the nodes are not willing to forward packets for the benefit of other nodes. This problem may arise in civilian applications of mobile ad hoc networks. In order to stimulate the nodes for packet forwarding, a simple mechanism based on a counter in each node. The behavior of the proposed mechanism analytically and by means of simulations, and detail the way in which it could be protected against misuse.

The problem of stimulating cooperation in self-organizing, mobile ad hoc networks for civilian applications is a major concern. Each node belongs to a different authority, its user, which has full control over the node. In particular, the user can tamper with the software and the hardware of the node, and modify its behavior in order to better adapt it to her own goals The regular users usually do not have the required level of knowledge and skills to modify their nodes. Nevertheless, our assumption is still reasonable, because criminal organizations can have enough interest and resources to reverse engineer a node and sell tampered nodes with modified behavior on a large scale. The experience of cellular networks shows that as soon as the nodes are under the control of the end-users, there is a strong temptation to alter their behavior in one way or another.

One approach to solve this problem would be to make the nodes tamper resistant, so that the behavior cannot be modified. However, this approach does not seem to be very realistic, since ensuring that the whole node is tamper resistant may be very difficult, if not impossible. Therefore, the approach requires only a tamper resistant hardware module, called security module, in each node. One can think of the security module as a smart card or as a tamper resistant security co-processor. Under the assumption that the user can possibly modify the behavior of the node, but never that of the security module, our design ensures that tampering with the node is not advantageous for the user, and therefore, it should happen only rarely[5].

The secure incentive protocol follows Tamper Proof Device Based Model. A TPD is installed in each node to store and manage its credit account and secure its operation. The self-generated and forwarded packets by a node are passed to the TPD to decrease and increase the node's credit account, respectively. Packet purse and packet trade models have been proposed. For the packet purse model, the source node's credit account is charged the full payment before sending a packet, and each intermediate node acquires the payment for relaying the packet. For the packet trade model, each intermediate node runs an auction to sell the packets to the next node in the route, and the destination node pays the total cost of relaying the packets.

The TPD-based payment schemes suffer from the following serious issues. First, the assumption that the TPD cannot be tampered with, cannot be guaranteed because the nodes are autonomous and self-interested, and the attackers can communicate freely in an undetectable way if they could compromise the TPDs. Second, the nodes cannot communicate if they do not have sufficient credits during the communication time. Unfortunately, the nodes at the net-work border cannot earn as many credits as the other nodes because they are less frequently selected by the routing protocol. Finally, since credits are cleared in real time, the multihop communications fail if the network does not have enough credits circulating around because the nodes do not have sufficient credits to communicate[6].

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. after receiving a data packet, the destination node sends a RECEIPT packet to the source node to issue a REWARD packet to increment the credit accounts of the intermediate nodes. The credit account of the source node is charged and a signature is attached to each data packet. Upon receiving the packet, the credit account of the destination node is also charged, and a digitally signed acknowledgement packet is sent back to the source node to increase the credit accounts of the intermediate nodes. The receipt-based payment schemes impose more over-head than the TPD-based schemes because they require submitting receipts to the AC and processing[7].

In a Report-based pAyment sChemE for MWNs the nodes submit light-weight payment reports to the AC to update the credit accounts, and temporarily store undeniable security tokens called evidences. The reports contain the alleged charges and rewards of different sessions without security proofs. 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. 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. Evidence aggregation technique is used to reduce the storage area of the Evidences[1].

III. Proposed Method

The trust based micro payment scheme can be described in five phases.

- Communication Phase
- Classifier Phase
- Identifying Cheater Phase
- Maintaining Trust based protocol
- Credit Account Update Phase

3.1 Communication Phase

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

Route Establishment : In order to establish an end-to-end route, the source node broadcasts the Route Request packet containing the identities of the source and the destination nodes, time stamp, and Time-To-Live . TTL is the maximum number of intermediate nodes. After a node receives the RREQ packet, it appends its identity and broadcasts the packet if the number of intermediate nodes is fewer than TTL. The destination node composes the Route Reply packet for the nodes broadcasted the first received RREQ packet, and sends the packet back to the source node. The RREP packet contains the identities of the nodes in the route, hash function h, and the destination node's certificate and signature.

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 M_X and its signature to R, X, Ts, and the hash value of the message and sends the packet to the first node in the route. The source node's signature is an undeniable proof for transmitting X messages and ensures the message's authenticity and integrity. Signing the hash of the message instead of the message can reduce the Evidence size because the smaller-size is attached to the Evidence instead of M_X. Before relaying the packet, each intermediate node verifies the signature to ensure the message's authenticity and integrity, and verifies R and X to secure the payment. Each node stores only the last signature for composing the Evidence, which is enough to prove transmitting X messages. The data transmission process ends when the source node transmits its last message, or if the route is broken due to node mobility or channel impairment.

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. Fig. 3.a gives the general format of an Evidence. The figure shows that an 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 nodes' signatures. From Fig. 3.a the DATA contains the identities of the nodes in the route , the number of received messages , the session establishment time stamp, the root of the destination node's hash chain , the hash value of the last message, and the last received hash value. 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.

$$DATA = R, X, Ts, H(M_X), h^{(0)}, [h^{(V)}]$$

$$PROOF = H(Sig_S(R, X, Ts, H(M_X)), Sig_D(R, Ts, h^{(0)}))$$

Fig. 3.a The General Format of Evidence

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.

Reducing the storage area of the Evidences is important because they should be stored until the AC clears the payment. Onion hashing technique can be used to aggregate Evidences. The underlying idea is that instead of storing one PROOF per session, one compact PROOF can be computed to prove the credibility of the payment of a group of sessions.

Payment report composition or submission : A payment report contains the session identifier, a flag bit, and the number of messages. The session identifier is the concatenation of the identities of the nodes in the session and the time stamp. The flag bit is zero if the last received packet is data and one if it is ACK. The submission of reports and Evidences are illustrated in and Fig.3.b.

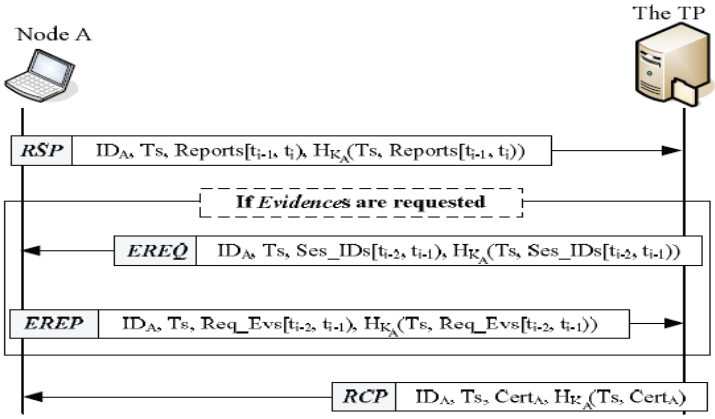

Fig 3.b The submission of reports and evidences

3.2 Classifier Phase

After receiving a session's payment reports, the AC verifies them by investigating the consistency of the reports, and classifies 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. Fair reports can be for complete or broken sessions. For a complete session, all the nodes in the session report the same number of messages and F of one. If a session is broken during relaying the Xth data packet, the reports of the nodes from S to the last node that received the packet report X and F of zero, but the other nodes report X _ 1 and F of one. If a session is broken during relaying the Xth ACK packet, the nodes in the session report X messages, and the nodes from D to the last node that received the ACK report F of one, but the other nodes report F of zero. The reports are classified as cheating if they do not achieve one of the aforementioned rules.

Case No.		**S**	**A**	**B**	**C**	**D**
1	X	11	11	11	11	11
	F	1	1	1	1	1
2	X	11	11	11	11	11
	F	0	0	1	1	1
3	X	8	8	7	7	7
	F	0	0	1	1	1
4	X	1	1	1	--	--
	F	0	0	0	--	--

Table 3.1 Numerical Example for Fair Report

Table 3.1 gives numerical examples for fair reports. Case 1 is reports for complete session and Cases 2 to 4 are reports for broken sessions. For Case 1, all the nodes report the same number of messages and F of one. For Case 2, the session was broken during relaying the ACK packet number 11 and B is the last node that received the packet. For Case 3, the session was broken during relaying the data packet number 8 and node A is the last node that received the packet. For Case 4, the session was broken during relaying the first data packet, and node B is the last node that received the packet, and therefore nodes C and D did not submit the payment report of the session.

3.3 Identifying Cheaters

In the Identifying Cheaters' phase, the TP processes the cheating reports to identify the cheating nodes and correct the financial data. Our objective of securing the payment is preventing the attackers from stealing credits or paying less, the attackers should not benefit from their misbehaviors. Guarantee should be there, that each node will earn the correct payment even if the other nodes in the route collude to steal credits. The AC 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 AC can precisely identify the cheating nodes with requesting few Evidences. To verify an Evidence, the TP

composes the PROOF by generating the nodes' signatures and hashing them. The Evidence is valid if the computed PROOF is similar to Evidence's PROOF.

3.4 Maintaining Trust based Protocol

In order to reduce the overhead and to provide more security the trust based protocol is implemented. Each nodes are assigned a trust value. Based on sending the packet successfully a trust value is assigned. The highest trust value is assigned for the nodes that relay messages more successfully. A trust based routing protocol is maintained to route the messages through the highly trusted nodes. It minimizes the probability of dropping the messages. The protocol helps to make smart decision regarding node selection with low overhead. When each node submits report to the accounting center the AC checks the consistency of the report. If it is consistent it is fair report. If it is inconsistent then AC ask the evidences. Upon processing the evidences the cheater nodes are identified and keep track of the cheater nodes and fair nodes separately. The routing protocol finds the possible short distance route from the highest trust valued nodes. It avoids the submission of inconsistent reports and the processing overhead for those inconsistent reports.

3.5 Credit Account Update

The Credit Account Update phase receives fair and corrected payment reports to update the nodes' credit accounts. In receipt-based payment schemes, a receipt can be cleared once it is submitted because it carries undeniable security proof, but the AC in RACE has to wait until receiving the reports of all nodes in a route to verify the payment. The maximum payment clearance delay occurs for the sessions that are held shortly after at least one node contacts the AC and the node submits the report after the certificate lifetime, at least one report is submitted after T_{Cert} of the session occurrence. It is worth to note that the maximum time duration for a node's two consecutive contacts with the TP is T_{Cert} to renew its certificate to be able to use the network.

IV. Conclusion

In the Trust based Payment Scheme the mobile nodes are assigned a trust value. Based on the trust value the routing is performed. Trust value is assigned based on relaying packet successfully. Each node submits a light weight report to the accounting center. The classifier checks the consistency of the report and classifies it into fair and cheating report. The payment of the fair reports is cleared. For the cheating report the Evidence is requested. Upon doing the cryptographic operations the cheating nodes are identified and evict those nodes from the payment and cheating count is maintained to modify the trust value. The payment is cleared for the fair nodes. The trust payment model enhances the fairness and connectivity during the communication. The numbers of submission of the inconsistent reports are very less. This reduces the processing overhead and clearance delay than the existing model.

References

[1] Mohamed M.E.A, 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, February 2013
[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, pp. 192-203, Jan. 2007
[3] 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, 319-332, 2006
[4] Y. Zhang and Y. Fang, "A Secure Authentication and Billing Architecture for Wireless Mesh Networks," ACM Wireless Net-works, vol. 13, no. 5, pp. 663-678, Oct. 2007.
[5] 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
[6] Y. Zhang, W. Lou, and Y. Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks," ACM Wireless Networks, vol. 13, no. 5, 569-582, Oct. 2007.
[7] A. Weyland, "Cooperation and Accounting in Multi-Hop Cellular Networks," PhD thesis, Univ. of Bern, Nov. 2005.