Middle-East Journal of Scientific Research 20 (11): 1651-1656, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.20.11.1928

Secure Incentive Protocol for Multi-Hop Wireless Network with Limited Use of Public Key Cryptography

R. Udayakumar, K.P. Thooyamani and V. Khanaa

School of Computing Sciences,
Bharath University, Chennai, India

Abstract: In multi-hop wireless networks, selfish nodes does not relay the packets that it received but it make use of the co-operative nodes to relay their packets. It may result in negative impact on network performance and fairness. Incentive protocol use credits to stimulate the selfish nodes to make them cooperative but existing protocol usually rely on heavy weight public operations to secure the payment In this paper, 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 next packets, so that the overhead of the packet series converges to that of the hashing operations Hash chains and keyed hash values are used to achieve payment non-repudiation and thwart free riding attacks. Security analysis and performance evaluation demonstrate that the proposed protocol is secure and the overhead is incomparable to the public key based incentives protocol. Because the efficient hashing operations dominate the nodes operation. The average packet overhead is less than that of the public-key based protocols with very high probability due to truncating the keyed hash values.

Key words: Mobile communication systems % Network-level security and protection % Payment schemes % Routing protocols

INTRODUCTION

In multi-hop networks a node's traffic is usually relayed through the other nodes to the destination nodes. Multi-hop relaying can enable new applications and enhance the network performance and deployment [1].

Advantages: It can extend the communication range using limited transmit power, improve area spectral efficiency and enhance the network throughput and capacity. Due to involvement of self-interested devices in the packet relay the routing process suffer from new security challenges that endangered the practical implementation of these networks. Hence this incentive protocol is used to motivate the selfish node to collaborate by proving that cooperation is more beneficial than the behaving selfishly. Reputation protocol is also implemented to mitigate the problems created by the selfish nodes.

Effects of Selfish Nodes: If 10% to 40% of the nodes are selfish then the average throughput degrades by 16% t0 32% and the delay increases linearly with the percentage of the selfish nodes.

Working of Incentive Protocol: Incentive-based protocols are more proper for multi-hop wireless networks because in addition to cooperation stimulation, these protocols can achieve fairness by rewarding credits to the cooperative nodes. These protocol can also used for billing the network services without contacting the distant home network register. Cooperative protocol is used as tamper proof device, electronic coin and central bank based protocols [2].

Related Work: In Nuglets, the self generated and forwarding Packets are passed to the tamper proof device to increase and decrease the credit account. CASHnet uses digital signatures operation. The extensive use of digital signature operations for both the data and ACK

Corresponding Author: Dr. R. Udayakumar, School of Computing Sciences, Bharath University, Chennai, India.

Table 1: Useful Notations.

CertS and CertD	The certificates of the source and the destination nodes
H(X)	Hash value resulted from hashing x
HKSi(X)	The hash value resulted from keyed hashing X using the key KSi
Idi	The identity of intermediate node i,or node with identity IDi
Ids and IDD	The identities of the source and the destination nodes, respectively
KSI	The key shared between the source and the intermediate nodes i
Mi	Message sent in the ith data packet
TS	The session establishment time stamp.

packet is not efficient for limited resource TPD based protocols suffer from following problems: it cannot be tampered is not secure for network with autonomous nodes and the attackers can communicate freely in undetectable way [3].

Issues in These Proposed Protocol: The proposed protocol in reduces the receipts' number by rewarding the nodes probabilistically. The source node appends a payment token to each packet and the intermediate nodes check whether the token corresponds to winning tickets that are submitted to the AC to reward the winning nodes. Instead of submitting the receipts by all the intermediate nodes, a receipt submission mechanism has been proposed in to reduce the number of submitted receipts and protect against collusion attacks. In addition, a hash chain is used to replace the destination node's signature with hashing operation, but signature operations are used for the data packets [4].

Network Architecture: The considered multi-hop wireless network includes an AC, a set of base stations and mobile nodes. The AC generates the required cryptographic credentials for a node to participate in the network and stores and manages the nodes' credit accounts. It updates the accounts of relevant nodes. For the payment model, a fair charging policy is to support cost sharing between the source and the destination nodes because both of them benefit from their communication. The AC charges the two communicating nodes for every transmitted packet even if the packet does not reach the destination node, but the AC rewards the intermediate nodes only for delivered packets. For fair rewarding policy, the value of **9** is determined to compensate the nodes for the consumed resources in relaying route establishment packets, packet retransmission and undelivered packets [5].

Overview and Contributions: A practical incentive protocol should achieve two essential requirements: lightweight overhead and security. Heavy overhead protocol degrades the network performance and exhausts the nodes' resources, which stimulates the nodes to behave selfishly. The public-key operations require much more complicated computations than the hashing operations the nodes' resources, which stimulates the nodes to behave selfishly. The public-key operations require much more complicated computations than the hashing operations. Therefore, if we can replace the public-key operations with hashing operations and reduce the packet overhead, the network performance can be improved significantly. the public-key operations require much more complicated computations than the hashing operations, in it will be shown that the verifying and signing operations require computation times and energy that are equivalent to (1061 and 927) and (1119 and_1038) hashing operations using DSA and MD5, respectively. In addition, secure public key cryptosystems usually have long signature tags which increase the packet overhead. Therefore, if we can replace the public-key operations with hashing operations and reduce the packet overhead, the network performance can be improved significantly.

Comparing with signature-based protocols, ESIP invests more overhead in the first data packet, but from the second packet, only the lightweight,hashing operations are used, so for a group of packets, the heavyweight overhead of the first packet vanishes and the overall overhead converges to the lightweight overhead of the hashing operations. it will be shown that the cryptographic delay in ESIP is 1.4 and 1.75 times that in DSA and RSA based incentive protocol for the first packet and for a series of two packets, the delay ratios drop to 0.68 and 0.88. Therefore, from the second packet, we gain the revenue of the investment from the first packet. Moreover, for a group of 13 packets, ESIP requires only 10% and 12% of the cryptographic delay in DSA and RSA based protocols, respectively For the packet overhead, it is obvious that if the number of intermediate node is large the packet overhead will be long, so for the efficient implementation of ESIP, the keyed hash values are truncated significantly and each intermediate node drops its hash value. we will argue that the severe hash truncation is secure in our protocol. It will be shown that the average packet overhead in ESIP is less than that of the signature based protocols with very high probability, e.g., for a series of 10 packets, the data packet overhead in ESIP is 70% and 37% of that in the DSA and RSA based protocol, respectively.

The Proposed Esip: Our protocol includes three phases. In Setup Phase, a network node receives the necessary cryptographic data to participate in the network. In Communication Phase, the nodes are involved in communication sessions and the intermediate node saves the resultant payment receipts. In Receipt Redemption Phase, the nodes submit the receipts to the AC to redeem them.

Setup Phase: Each node stores a unique identity and public/private key pair with a certificate, the public key of the AC and the required cryptographic data for the key exchange protocol. As shown in Fig. 1, each node on a session has to share a symmetric key with the source node to compute the messages' keyed hash values. For efficient implementation, an identity-based key exchange protocol based on bilinear pairing can be used because the nodes do not need to exchange messages to compute the shared keys. The AC generates a prime p, a cyclic additive group (G) and a cyclic multiplicative group (GT) of the same order p such that an efficiently computable bilinear pairing ê: G × G _GT is known. The bilinear mapping has the following properties:

Bilinear: ê(a • P, b • Q) = ê(b • P, a • Q) = ê(P, Q)a • b, for all

P, Q G and a, b ZP
*.

Non-degeneracy: ê(P, Q) z 1GT.

Symmetric: ê(P, Q) = ê(Q, P), for all P, Q G.

Admissible: there is an efficient algorithm to compute ê(P, Q) for any P, Q G.

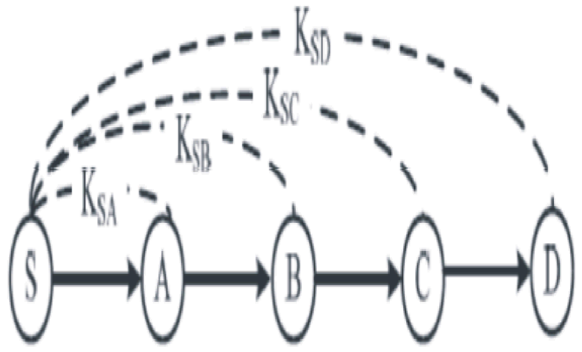


Fig 1: The Source Node Shares a Key with Each Node in the Rourte

The bilinear map ê can be implemented efficiently using the Weil and Tate pairings on elliptic curves The AC selects a random element P ZP * known as the master key and computes the secret keys for the nodes based on their identities. The secret key for node IDi is Ski = P_•_H(IDi) G, where

H: {0,1}* _G. Two nodes with identity/secret key pairs (IDS, SKS) and (IDA, SKA) can independently compute the shared key as follows:

KSA = ê(H(IDA), SkS)

= ê(H(IDA), P_• H(IDS))
= ê(P_• H(IDA), H(IDS)) (Bilinear property)
= ê(SkA, H(IDS))
= ê(H(IDS), SkA) (Symmetric property)
= KAS

Communication Phase: Route Request Packet (RREQ) that contains its identity (IDS), time stamp (TS) and the identity of the destination node (IDD) and the time to live (TTL). If the time stamp is within a proper range and the TTL is not zero, a network node decrements the TTL, appends its identity and broadcasts the packet.The source and the destination nodes generate hash chains by iteratively hashing. Then it verifies its message's truncated hash value to ensure the message's authenticity and integrity and relays the packet after dropping its hash value. to ensure that it will be rewarded for relaying the packets. Then it verifies its message's truncated hash value to ensure the message's authenticity and integrity and relays the packet after dropping its hash value.

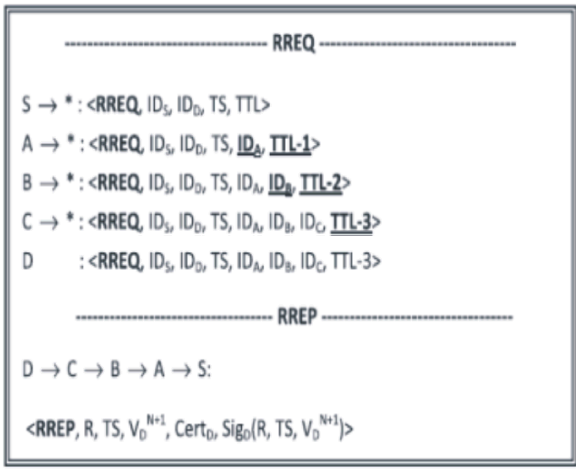


Fig 2: Route Establishment Packets

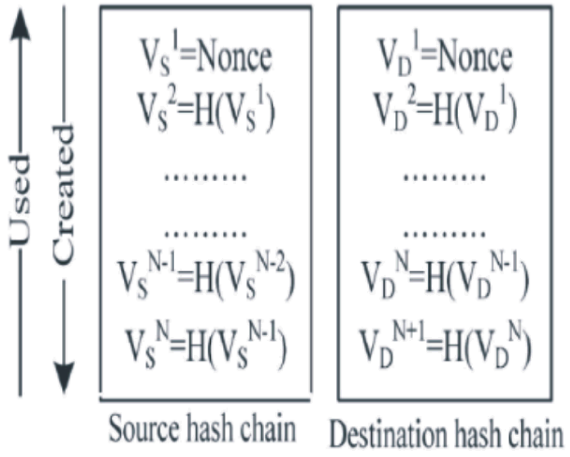


Fig 3: The Source and Destination Nodes Hash Chains

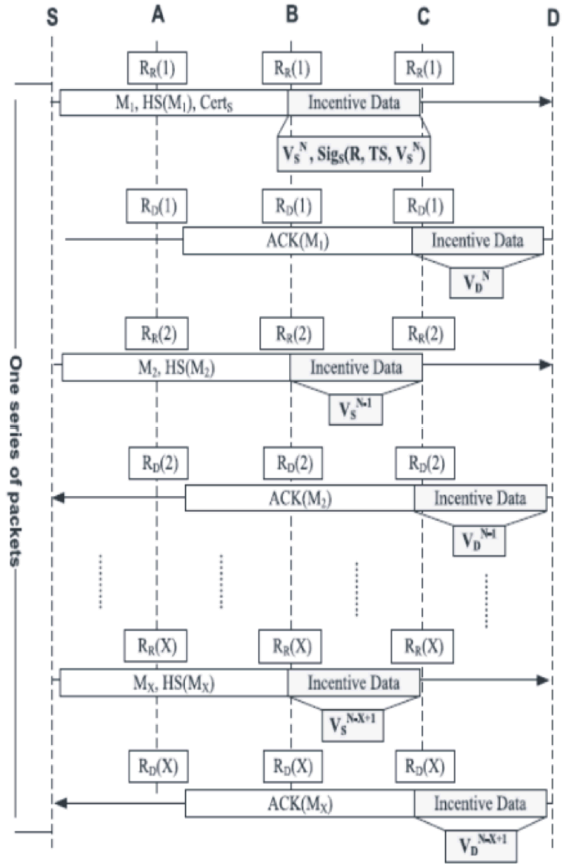


Fig 4:

Each intermediate node saves the source node's signature and VSN to be used in receipt composition.

As shown in Fig. 5, for the successive packets (X > 1), the source node appends the pre-image of the last sent hash value (VSN-X+1) as an approval to pay for one more packet and the truncated hash series (HS(MX)). Each intermediate node verifies its message's truncated keyed hash value, verifies that VS N-X+1 is generated from hashing VS N-X and relays the packet after dropping its hash value. Each intermediate node saves the last received hash value (VS N-X+1) to be used in receipt composition.

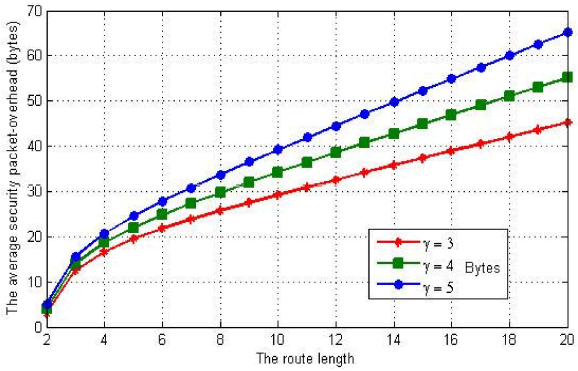
Payment Redemption Phase: The network nodes periodically submit the receipts to the AC to redeem them. Once the AC receives a receipt, it first checks that the receipt has not been deposited before using the receipt's unique identifier, i.e., the identities of the nodes on the route and the establishment time (R, TS). Then, the AC verifies the receipt credibility by generating the source and the destination nodes' signatures and matching the signatures' hash value with the receipt's security token. Finally, the AC counts the packets' number from the hash chain's elements and clears the receipt according to the rewarding and charging policy.

Security Analysis: To simplify our presentation, we considered that a keyed hash value covers only the message, but for better security, it should cover the whole packet., the keyed hash value of node B should be HKSB(MX, VSN-X+1, HKSC(MX), HKSD(MX)), so if node A manipulates the hash value of D, e.g., to consume the nodes' resources because the packet will be dropped at D, node B can stop propagating the incorrect packet. Since the source node attaches a keyed hash value for each node on the route, it is obvious that the packet overhead will be large for long routes. To reduce the packet overhead, the message's keyed hash value can be truncated significantly, e.g., the size of the truncated hash value (J) can be 4 or 5 bytes instead of 16 bytes in HMAC-MD5. This severe hash truncation is secure in our protocol for the following reasons: (1) The packet security lifetime is extremely short, i.e., if an intermediate node does not relay a packet in a short time, the route is considered broken and re-established, so a malicious node does not have long time to run complicated algorithms to figure out the truncated keyed hash values for the manipulated message; (2) Without knowing the secret key, computing the keyed hash value is difficult; and (3) An attacker has to figure out a keyed hash value for each victim between itself and the other colluder. Therefore, an attacker has to compute multiple truncated keyed hash values without knowing the keys in a limited time, which is so difficult. What an attacker can do is to replace the truncated hash with a random value, but the probability to hit the correct value is extremely low, e.g.,

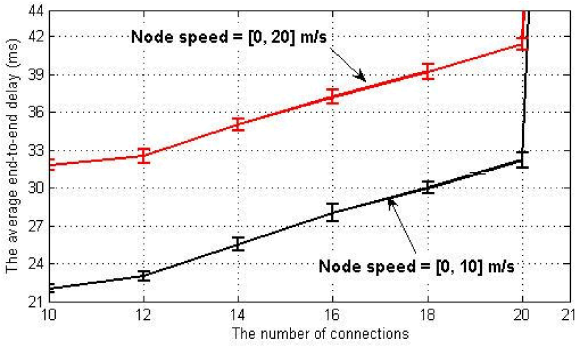
for J_= 4 bytes, the probabilities to hit one and two correct hash values are 0.23¯10-9 and 0.05¯10-18, respectively. However, hash truncation increases the random collision probability, i.e., the corrupted and the original messages have the same truncated keyed hash value. Using birthday paradox, the random collision probabilities for J of 4 and 5 bytes are 1.2¯10-5 and 7.63¯10-7, respectively. In addition, since message integrity is checked in each hop, the probability that the destination node falsely accept a corrupted message as correct is (n1¯1.2¯10-5) for J of 4, which is equivalent to the probability that hash collision occurs in n1 successive nodes, where n1 is number of nodes from the node at which the message is corrupted to the destination node. This probability can be reduced with the increase of J but the packet overhead increases, so J can be dynamic to balance between the probability of falsely accepting corrupted message and the packet overhead, i.e., J can be longer for short routes. Moreover, some nodes on the route can have longer J than others, e.g., J can be longer for the destination node to prevent falsely accepting corrupted messages. MD5 is faster and has shorter digest length than SHA-2, but SHA-2 is more collision resistant, so SHA-2 can be used in signing operations that require high collision resistance,and MD5 is used to compute the keyed hashes and the hash chain.

Performance Evaluation: In this section, simulation results are given to evaluate the overhead cost and the expected network performance using ESIP.

Simulation Setup: We use 1024-bit RSA and 1024-bit DSA with signature tags of 128 and 40 bytes, respectively, because the secure private keys should have at least 1024 bits according to NIST guidelines For the hash functions, we use MD5 and HMACMD5 with digest length of 16 bytes. For the pairing operation, we consider the Tata pairing implementation on MNT curves where *G* is represented by 171 bits and the order *P* is represented by 170 bits. The discrete logarithm in *G* is as hard as the discrete logarithm in Zp * where *P* = 1024 bits. Network simulator NS2 is used to implement ESIP and signature-based protocol that uses public-key operations in each packet. We simulate multi-hop wireless network by randomly deploying 35 mobile nodes in a square cell of 800 m × 800 m. The Distributed Coordination Function (DCF) of IEEE 802.11 is implemented as the medium access control (MAC) layer protocol. The radio transmission range of a node is 125 m and the transmission data rate is 2 Mbits/s. A node movement is simulated using the random waypoint model [33] with speed and pause times uniformly distributed in the ranges [0, 10] m/s and [0, 50] s, respectively. Specifically, a node travels towards a random destination uniformly selected within the network field; upon reaching the destination, it pauses for some time; and the process repeats itself afterwards. The constant bit rate (CBR) traffic source is implemented in each node and the source and destination pairs are randomly chosen. All the data packets are 512 bytes and sent at rate of 2 packets/s. The time stamp and an identity are five and four bytes, respectively. Each simulation is performed 50 runs and each run is executed for 15 simulated minutes of five.



The average packet security-overhead in ESIP.



The impact of mobility on the end-to-end packet delay.

CONCLUSION

In this work, we have implemented virtual currency in the multi-hop wireless network to stimulate the rational packet droppers to cooperate. However, the irrational packet droppers, e.g., compromised or faulty nodes, sacrifice their resources such as energy, bandwidth, credits, etc to harm the network, i.e., they attempt to degrade the network performance by involving themselves in communication sessions and then dropping the packets intentionally. Since the sessions may be

broken normally, e.g., due to mobility, or intentionally due to malicious actions, statistical methods are required to identify the irrational attackers that drop the packets more than the normal rate. In ESIP, the receipt format can reveal the node at which the route was broken, so in our future work, we will extend this work to consider the irrational packet droppers. The AC can inspect the submitted receipts to build a reputation system to identify the irrational packet droppers. The reputation system should be carefully designed to identify the attackers in short time to reduce their harm and to avoid falsely identifying honest nodes as irrational packet droppers.

REFERENCES

1. Mohamed Elsalih Mahmoud and Xuemin (Sherman) Shen, 0000. Fellow, IEEEESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-hop Wireless Networks.
2. Xie, L. and S. Zhu, 2008. Message dropping attacks in overlay networks: attack detection and attacker identification, ACM Transactions on Information and System Security, 11(3).
3. Zhang, Y. and Y. Fang, 2007. A secure authentication and billing architecture for wireless mesh networks, ACM Wireless Networks, 13(5): 569-582.
4. Buttyan, L. and J. Hubaux, 2001. Nuglets: a virtual currency to stimulate cooperation in self organized ad hoc networks, Technical Report DSC/2001/001, Swiss Federal Institute of Technology, Lausanne.
5. Buttyan, L. and J. Hubaux, 2004. Stimulating cooperation in self-organizing mobile ad hoc networks, Mobile Networks and Applications, 8(5): 579-592.