A Privacy-Preserving Routing and Incentive Protocol using Lightweight Approach for Hybrid Ad Hoc Wireless Network

Anjan Baradwaj S, Naveen H R, Harish P, Praveen Kumar T S
City Engineering College, Karnataka, Bangalore, India

Abstract

We propose a privacy-preserving routing and incentive protocol for hybrid ad hoc wireless network. This protocol uses credit schemes to stimulate a nodes cooperation. Lightweight hashing and symmetric-key-cryptography operations are implemented to preserve the privacy of users. The node's pseudonyms are computed efficiently using hashing operations. Only a trusted party can link these pseudonyms to the real identities. Moreover, this protocol also protects the location privacy of the anonymous source and destination nodes. Analysis and simulation experiments demonstrate that this protocol can secure the payment and preserve the user's privacy with acceptable overhead.

1. Introduction

In hybrid ad hoc wireless network, the mobile nodes usually act as routers to relay other's traffics for enhancing the network performance and deployment [1]. Multi-hop packet relay extends the base station's coverage area without additional cost. It also enhances the throughput and capacity of the network due to reduction of the transmission interference area by transmitting the packets over shorter hops. However, the nature of the wireless transmission and multi-hop packet relay makes the network highly vulnerable to serious security challenges.

Although the proper network operation requires the node's cooperation in relaying others' packets, the selfish nodes will not cooperate without sufficient incentive to save their resources. This behavior degrades the network connectivity and packet delivery ratio and may result in failure of the multi-hop communication [2]. Moreover, the attackers can analyze the network traffic to learn the user's locations in number of hops and their communication activities which might be a severe threat for the users' privacy. These attacks can be launched in undetectable manner because the attackers just overhear the transmissions without disturbing the communication. schemes discourage launching Resource- Exhaustion attack by sending bogus messages to exhaust the node's resources.

However, each node has to use a unique identity in the existing schemes for charging and rewarding operations, which jeopardizes the user's privacy. They also incur much overhead due to the use of public key cryptography and submitting receipts (proofs of packet relay) to a trusted party (Tp). Moreover, the existing privacy-preserving routing protocols [7-9] heavily depend on packet broadcasting and public key cryptography, which makes these protocols infeasible for hybrid ad hoc networks due to the constraints on the node's resources.

In this paper, we propose a protocol for hybrid ad-hoc wireless network. This protocol can foster node cooperation and preserve the privacy of the user's locations and communication activities using lightweight hashing and symmetric-key-cryptography operations. The pseudonyms of the nodes are efficiently computed using hashing operations. Only trusted parties can link these pseudonyms to the real identities for charging and rewarding operations.

2. System Model

2.1 Network Model

The considered hybrid ad hoc wireless network consists of mobile nodes, a set of base stations, and Tp. The base stations are connected with each other and with Tp by a backbone net- work. A mobile node X should register with Tp to get a permanent shared symmetric key K_X and a unique identity ID_X. Tp manages the node's credit accounts and maintains their keys. The source node (S) sends its packets to the source base station (Bs), if necessary in multiple hops. Bs forwards the packets to the destination base station (Bd) if the destination node (D) resides in a different cell, and finally, the packets are sent to D, possibly in multiple hops again. The part of the route between S and Bs is called uplink and the part of the route between Bd and D is called downlink.

Our payment model supports a cost sharing between the source and the destination nodes when both of them benefit from the communication. The payment-splitting ratio is adjustable and service-dependent, e.g., a DNS server should not pay for name resolution. The source and the destination nodes are charged and the uplink intermediate nodes are rewarded only for the messages received by Bs even if they do not reach to D. The downlink intermediate nodes are rewarded only when Bd receives Acknowledgement packet (ACK) from D.

2.2 Threat and Trust Models

The attackers have full control on their nodes and thus they can change the node's operations. The attackers work individually or collude with each other to launch sophisticated attacks. Specifically, the attackers attempt to steal credits, pay less, and communicate freely. Legitimate nodes or eavesdroppers may attempt to learn the nodes' real identities and locate individual nodes in number of hops and track their movements. The attackers also aim to launch traffic analysis attacks to monitor communication activities of nodes. However, Tp and the base stations are secure because they are operated by a single operator that is motivated to ensure the network security. The node's real identities and location are known to the base station and Tp in order to route the messages accordingly. Nevertheless, the node's long term keys are known only to Tp. We do not consider the global eavesdropper that can monitor every radio transmission on every communication link in the network at all time. This is because these attacks are too complicated to occur in civilian applications and scalable net- works, and the countermeasures usually require much over- head. In this protocol, the global eavesdroppers may locate the source and destination nodes and identify the route if there is only one active session in the network, but they cannot link the nodes' pseudonyms to the real identities. For the trust models, the nodes trust Tp and the base stations with performing billing and auditing correctly and with preserving their location and identity privacy, but they do not trust the mobile nodes.

.

.

3. The Proposed Protocol

3.1. Pseudonyms and Shared Keys

To protect a node's identity privacy, the node uses pseudonyms such that only an intended node can link the pseudonyms to each other and to the real identity.

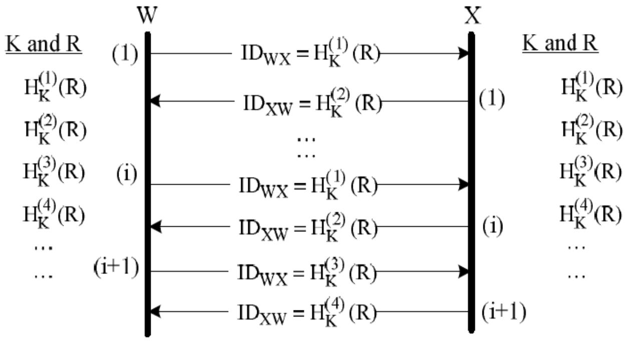


Fig. 1: Pseudonyms generation technique.

In this way, even if an attacker could link a pseudonym to a node, he cannot violate the node's privacy for a long time. As shown in Fig. 1, if the nodes W and X share a secret key K and a public seed R, they can generate shared pseudonyms by iteratively keyed hashing R, where $H_K^{(n)}$ (R) refers to the message authentication code resulted from iteratively hashing R n times using the key K. The hash values generated from hashing R with odd numbers ($H_K^{(1)}$ $H_K^{(3)}$ etc.) are used by node W and those generated from hashing R with even numbers ($H_K^{(2)}$ $H_K^{(4)}$ etc.) are used by node X. The frequency of pseudonym change (i) is the number of packets that use one pseudonym, e.g., each pseudonym is used only for one packet if i is one. In order to keep pseudonym synchronization between W and X, each node compares a packet's pseudonym with the current and next pseudonyms. For example, in the packets (1 to i), W compares X's pseudonym to $H_K^{(2)}$ and $H_K^{(4)}$(R). Moreover, a node does not change its pseudonym more than once before the other node changes its pseudonym. In this way, if packet (i+1) is lost, the nodes do not lose synchronization because W does not use $H_K^{(5)}$ before receiving $H_K^{(4)}$ from X. After X receives $H_K^{(2)}$, it knows that W wants to change pseudonym and thus it also changes its pseudonym by sending $H_K^{(4)}$. The main advantage of this pseudonym generation technique is that the nodes do not have to change their pseudonyms at a fixed frequency. Pseudonym change can be arbitrarily triggered by X or W without losing synchronization. .

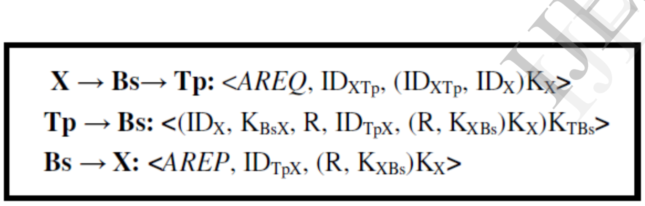
A pseudonym generation requires only one lightweight hashing operation and does not require large storage area or frequently contacting Tp to re-fill pseudonyms. This enables the nodes to reduce the lifetime of each pseudonym to improve the user's privacy. Pseudonyms can also be computed before receiving a

This protocol requires three types of symmetric keys and pseudonyms:-

1) Node-to-Tp: Node X and Tp share a long-term key K_X. Using this key, they can generate a long term pseudonyms ID_{XTp} and $ID_{TpX.}$

2) Node-to-Base Station: Each node shares a symmetric key and pseudonyms with its cell's base station. Once the node leaves the cell, the key and the pseudonyms become invalid. When node X first joins a new cell, Tp mutually authenticates the node and the cell's base station.

As shown in Fig.2, node X sends an Authentication Request (AREQ) packet containing a pseudonym shared with Tp (ID_{XTp}) and the encryption of its real identity and ID_{XTp}, where (M)K refers to the ciphertext resulted from encrypting M with K. AREQ authenticates X to Tp because the secret key KX is required to compose the packet. Tp replies with the node's real identity, the shared key between X and Bs ($K_{XBs} = K_{BsX}$), and the seed of the pseudonyms (R). R and K_{XBs} are used to generate pseudonyms shared between X and Bs. In this way, Tp mutually authenticates X and Bs without revealing the node's long-term secret key.



X → Bs→ Tp: $<AREQ, ID_{XTp}, (ID_{XTp}, ID_X)K_X>$

Tp → Bs: $<(ID_X, K_{BsX}, R, ID_{TpX}, (R, K_{XBs})K_X)K_{TBs}>$

Bs → X: $<AREP, ID_{TpX}, (R, K_{XBs})K_X>$

Fig.2 Authentication Phase

3.2. Route Establishment Phase

As shown in Fig. 3, S broadcasts an Uplink Route Request (URREQ) packet that is forwarded by Bs to Bd if D resides in a different cell. Bd broadcasts the Downlink Route Request (DRREQ) packet and D sends back the Route Reply Packet (RREP) packet. Finally, Bs and Bd send the Uplink and the Downlink Route Establishment packets (UREST and DREST) to establish the uplink and the downlink route

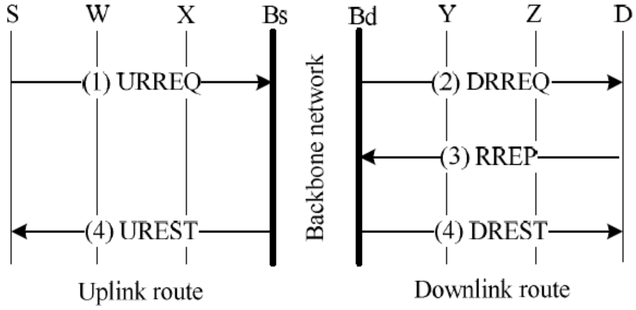


Fig. 3: Route Establishment phase.

4. Security Analysis

4.1. Defense against Payment Manipulation

The iterative encryption/decryption operations can protect against several attacks. First, removing the encryptions and verifying the correctness of the resulting packet implicitly authenticates the intermediate nodes and ensures that the packet is relayed through the route it was supposed to take. Second, in Free-Riding attacks, two colluding nodes C1 and C2 in a legitimate session manipulate the session packets to add their data to communicate freely. The iterative encryption/decryption operations can thwart the attack because the data sent by C1 cannot be interpreted by C2 because it is encrypted (or decrypted) by at least one intermediate node. Third, the iterative encryption/decryption operations make the packets look different as they are relayed, which makes packet likability and tracing not possible.

For Packet-Replay attack, the internal and external attackers may record valid packets and replay them in different place and/or time claiming that they are fresh to establish sessions under the name of others to communicate freely. If the attacker replays the URREQ packet, he cannot establish the session because he cannot generate a fresh pseudonym or de-crypt the UREST packet to get the key shared with his neigh- bor. In addition, since the source node encrypts a time stamp in the URREQ packet, the attacker cannot send valid packets without knowing a secret key because the packets are eventually dropped at the base station.

For Impersonation attack, the attackers attempt to impersonate other nodes to communicate freely. This attack is not possible in this protocol because the nodes have to authenticate themselves using the long-term keys shared with Tp in order to share a key with the base station. For Man-in-the-Middle at- tack, the attacker residing between a node and Tp may attempt to get the key shared between the node and the base station to communicate freely under the name of the node. This protocol is not vulnerable to this attack because the shared key with the base station is encrypted with the node’s long-term key.

For Destination-Node-Robbery attack, the source node colludes with some intermediate nodes to steal credits from the destination node by sending bogus data. In this protocol, the inter- mediate nodes are rewarded only when the destination node acknowledges receiving correct data, and the session cannot be established if the destination node is not interested in the communication because it has to send the RREP packet. For Credit-Overspending attack, the nodes may spend more than the amount of credits they have at the time of the communication. Most of the existing incentive schemes [3-6] are vulnerable to this attack because they use post-paid payment policy, i.e., the nodes communicate first and pay later. This protocol is not vulnerable to this attack because the base stations know the nodes’ total credits from Tp during authentication phase and do not allow the nodes to overspend their credits.

Although, the charges are always more than or equal to the rewards, the payment model does not make credits disappear because purchasing credits for real money can compensate the credit loss. The payment model can encourage node cooperation and counteract cheating actions without submitting payment receipts as follows:

1) The nodes are motivated to relay the data packets because the nodes are rewarded only when the packets are delivered;

2) Relaying the route establishment packets is beneficial for the nodes to participate in a session and thus earn credits. Relaying the ACK packets can trigger the source node to generate more packets and thus earn more credits. It is also beneficial for the downlink nodes because they are rewarded only when the ACK packets reach to Bd; and

3) If the nodes are charged only when the destination node receives a message, the node may claim that it does not receive the message in order not to pay. To prevent this, both S and D are charged for un-delivered messages.

6. Performance Evaluation

6.1. Cryptographic Overhead

To evaluate the computational time of the cryptographic operations used in this experimental study, AES symmetric key cryptosystem and SHA-1 (160 bit) hash function are implemented using Crypto++ library [10]. The secure key size is at least 128 bits according to NIST [11]. The mobile node is a laptop with an Intel processor at 1.6 GHZ (CPU) and 1.00 GB Ram, and Windows XP operating system. The results demonstrate that a hashing operation requires 16.79 Megabytes/s and encryption and decryption operations require 9.66 Megabytes/s. these results are scaled by the factor of ten to emulate a limited re- source node. For the energy consumption, it is shown in [12] that a hashing operation requires 0.76 J/byte and encryption and decryption operations require 1.21 J/byte.

6.2. Communication Overhead

This protocol was simulated using a network simulator written in MATLAB. 35 mobile nodes are randomly deployed in a square cell of 1000 m × 1000 m, and a base station is located at the center. The radio transmission range of the mobile nodes and the base station is 125 m. The random waypoint model is used to emulate the node mobility. The node speed is uniform- ly distributed in the range [0, 3] m/s and the pause time is 20 s. The constant bit rate traffic source is implemented in each node as an application layer. The source and destination pairs are randomly selected. The packets are sent at the rate of 2 packets/s. Distributed Coordination Function (DCF) of IEEE 802.11 is simulated as a medium access control (MAC) layer protocol. Our simulation is executed for 15 minutes and the results represent the average of 50 runs. The pseudonyms can be truncated into shorter length without significantly increasing the probability of pseudonym collision. The length of the truncated pseudonym (δ) depends on the cell size and the number of nodes in the cell. δ can be frequently computed by the base station and broadcasted. The length of δ, Pad, time stamp, real identity, and M_C are 10, $2 \cdot \delta$, 5, 4, and 512 bytes, respectively.

The simulation results given in Table 1 indicate that the expected delay is acceptable due to lightweight cryptographic operations. The average length of the URREQ packet is computed by dividing the amount of relayed data in all links by the number of links. The simulation results show that only 24-byte packet overhead are added to each message.

Table 1: Simulation results

	URREQ	RREP	DREST	Data Packet
Avg. packet length (bytes)	73.68	95.31	170.27	534
Avg. delay (ms)	19.3647	21.351	21.242	32.7612

7. Conclusion and Future Work

We have proposed a privacy-preserving routing and incentive protocol for hybrid ad hoc wireless network. Micropayment is used to stimulate node cooperation without submitting receipts. Our protocol can achieve a high protection level for user privacy using lightweight cryptographic tools. For efficient generation of pseudonyms, only the lightweight hashing operations are required. Extensive evaluations and simulations demonstrate that node cooperation and privacy preservation can be securely and efficiently integrated in one protocol.

Similar to the existing incentive schemes, this protocol thwarts selfishness attacks but cannot identify the malicious nodes that drop packets to launch Denial-of-Service attacks. The base stations can inform Tp how frequently the nodes drop the packets. However, packets can be dropped normally, e.g., due to mobility, or maliciously, but the high frequency of packet drop is an obvious malicious behavior. In our future work, we will study how Tp can precisely differentiate between honest and malicious nodes.

REFERENCES

[1] A. Abdrabou and W. Zhuang, “Statistical QoS routing for IEEE 802.11 multihop ad hoc networks”, IEEE Transactions on Wireless Communica- tions, vol. 8, no. 3, pp. 1542 - 1552, March 2009.

[2] K. Liu, J. Deng, and K. Balakrishnan, “An acknowledgement-based approach for the detection of routing misbehavior in MANETs”, IEEE Transaction on Mobile Computing, vol. 6, no. 5, May 2007.

[3] S. Zhong, J. Chen, and R. Yang, “Sprite: A simple, cheat-proof, credit based system for mobile ad-hoc networks”, Proc. of IEEE INFOCOM, vol. 3, pp. 1987-1997, San Francisco, CA, March 30- April 3, 2003.

[4] M. Mahmoud and X. Shen, “PIS: A practical incentive system for multi- hop wireless networks”, IEEE Transaction on Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, 2010.

[5] M. Mahmoud and X. Shen, “Stimulating cooperation in multi-hop wire- less networks using cheating detection system”, Proc. of IEEE INFOCOM, pp. 776–784, San Diego, CA, March 14–19, 2010.

[6] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, “Node cooperation in hybrid ad hoc networks”, IEEE Transactions on Mobile Computing, vol. 5, no. 4, pp. 365–376, April 2006.

[7] S. Capkun, J. P. Hubaux, and M. Jakobsson, “Secure and privacy- preserving communication in hybrid ad hoc networks”, Technical Report IC/2004/10, EPFL-DI-ICA, 2004.

[8] J. Kong and X. Hong, “ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks”, Proc. of ACM Mobi- Hoc, pp. 291-302, Annapolis, Maryland, USA, June 1-3, 2003.

[9] A. Boukerche, K. El-Khatib, L. Korba, L. Xu, “A secure distributed anonymous routing protocol for ad hoc wireless networks”, Journal of Computer Communications, NRC 47393, 2004.

[10] W. Dai, “Crypto++ Library 5.6.0”, http://www.cryptopp.com.

[11] National Institute of Standards and Technology (NIST), “Recommendation for key management - Part 1: General (Revised)”, Special Publication 800-57 200, 2007.

[12] N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, “A study of the energy consumption characteristics of cryptographic algorithms and se- curity protocols”, IEEE Transactions on Mobile Computing, vol. 5, no.2, pp. 128-143, March-April 2006.

[13] Mohamed Elsalih Mahmoud and Xuemin (Sherman) Shen, “Lightweight Privacy-Preserving Routing and Incentive Protocol for Hybrid Ad Hoc Wireless Network”, The First International Workshop on Security in Computers, Networking and Communications, 2001