Secure Communication for Lightweight Privacy-Preserving to Hybrid AD HOC Wireless Networks

Vidhya.D
Department of Information Technology, MAM College of Engineering, Trichy, Tamil Nadu, India

Article Info
Article history:
Received 3 February 2015
Received in revised form
20 February 2015
Accepted 28 February 2015
Available online 6 March 2015

Keywords
Payment System,
Pseudonym Generation,
Trapdoor Techniques,
One Time Session Kev

Abstract
To preserve user secrecy each node uses pseudonyms and session key for one time. In addition to secure the communication the system develops efficient pseudonym generation and trapdoor method requires only efficient lightweight hashing operations and a payment system. The fictitious will not require large storage area and refill the central unit frequently. The real challenge of privacy preserving protocol is each node has to use one authenticated identity for securing the protocol and the low overhead requirement contradicts with the large overhead usually needed for preserving privacy and securing the communication. The results of the Protocol can preserve privacy and secure the communication with low overhead.

1. Introduction

The most promising network in the base station is hybrid Ad hoc network. This has uplink, downlink and multihop. The uplink is an source node of base station and downlink is an destination of transmit packet. The multihop will extent the base station area by enabling the node outside the coverage area to use the network. The multihop will incrase the throughput for more efficient of bandwidth. With help of multihoping it transfer the packet over shorter hop in interference area. The packet over shorter hop in interference area. However included self ruling and self interested nodes in packet transmit and the broadcast nature of wireless tramsimision make network made highly danger to serious security and privacy abuse attack.

The third party will examine the network transmsion between two users. For example when, where, what etc. its effect will be hazard for the users privacy. Due to this the adversaries willtracket theorginial packet from source to destination. They may also find the users location and track their location. It will enlightening the user location for the physical attack. To Develop low overhead secure and privacy preserving communication protocol has a real challenges they are securing the protocol usually requires each node to use one authenticated identity but a permanent identity should not be used to preserve the nodes privacy and reducing the protocol overhead is necessary because the nodes are constrained by limited battery energy and computing power. To secure the communication the system use hashing and secret key cryptography operations and a payment system. The system uses credits to charge the nodes that send packets and reward those relaying them. Integrating privacy preservation with the payment system is essential to gain acceptance from the users to relay others packets. Although the payment can make a packet relay beneficial most users will not sacrifice their privacy for earning credits. To reduce the overhead protocols avoid the secret key cryptography because it consumes much resource increases the packet delivery delay and degrades the packet delivery ratio. The user develop efficient pseudonym generation technique that uses hashing operations. The low overhead of the hashing operations will facilitate reducing the lifetime of each pseudonym and thus boosting the user's privacy. The end to end packet delay can be reduced because pseudonyms are fast to compute and can be precomputed before receiving the packets. The pseudonyms are authenticated and always synchronized and do not require a large storage area or frequently contacting a central unit for refilling.

Corresponding Author,
E-mail address: vidhya111190@gmail.com

2. Proposed Scheme

Permanent identity should not be used to preserve the nodes privacy. Propose a efficient lightweight protocol for securing route establishment, data transmission and preserving users privacy in hybrid ad hoc wireless networks. To preserve users secrecy each node uses pseudonyms and single session key. New protocol enables the nodes to establish routes and send packets without revealing their real identities or the identity of the destination node. A nodes identity to pseudonyms can authenticate it to the intended nodes without revealing. So the attacker eavesdrops on both the source and destination nodes user cannot correlate their packets. Securing the protocol and preserve privacy the intermediate nodes can ensure that the packets are sent by legitimate nodes without revealing the real identities of the source and destination nodes without any receipts. So must build up efficient pseudonym generation technique that uses hashing operations. The low overhead of the hashing operations will facilitate reducing the lifetime of each pseudonym and thus boosting the users privacy. The end to end packet delay can be reduced because pseudonyms are fast to compute and can be pre-computed before receiving the packets. The pseudonyms are authenticated and always synchronized and do not require large storage area or frequently contacting a central unit for refilling for Secure Payment System. Some Proposed Techniques are Anonymous pseudonyms and one-time session key and Random Number Generation for secure key. The major advantages are an adversary captures a packet, he cannot infer the real identities of the source, destination, or intermediate nodes and cannot view original

Data and also reduce the overhead to avoids the asymmetric-key cryptography because it consumes much resource, increases the packet delivery delay and degrades the packet delivery ratio.

3. Related Works

[1]. Multihop relaying can enable new applications and enhance the network performance and deployment. A nodes traffic is usually relayed through other nodes to the destination. It can extend the communication range using limited transmit power improve area spectral efficienc and enhance the network throughput and capacity. Developing rural areas multihop wireless networks can be deployed more readily and at low cost. The communicating nodes pay credits to the intermediate ones to relay their packets. Reputation-based protocols suffer from unreliable detection to the selfish nodes because it is difficult to differentiate between a nodes unwillingness and incapability. For example due to low resources to cooperate. The existing protocols usually rely on the heavy weight public-key operations to secure the payment. 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.

To overcome this propose secure cooperation incentive protocol that uses the public key operations only for the first packet in a series and uses the efficient 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 incentive protocols because the efficient hashing operations dominate the nodes operations. Reputation and incentive based protocols have been proposed to mitigate the problems caused by the selfish nodes for reputation based protocols and each network node monitors the transmissions of its neighbors to make sure that the neighbors forward other nodes traffic and thus the uncooperative nodes can be identified and punished.

Propose an Efficient and Secure cooperation Incentive Protocol that uses public-key operations only for the first packet in a series, and then the efficient hashing operations are used in the next packets.

[2] A mobile station that has no direct connection with a base station can use other mobile stations as relays. Compared with conventional structure-based networks in new generation can lead to a better use of the available spectrum and to a reduction of infrastructure costs. The benefits would vanish if the mobile nodes did not properly cooperate and forward packets for other nodes and charging and rewarding scheme to encourage the most fundamental operation namely packet forwarding.

Use MAC layering to reduce the space overhead in the packets and a stream cipher encryption mechanism to provide implicit authentication of the nodes involved in the communication. Analyze the robustness of our protocols against rational and malicious attacks. The main are solution collaboration is rational for selfish nodes.

Collaboration cannot be taken for granted in a civilian network because each user wants to maximize his benefit while minimizing his contribution. Indeed to forward packet is energy consuming and a selfish user can tamper with his mobile device to remove the relaying functions or simply shut down the device when he is not using it. A systematic denial of the packet to be forwarding service would remove all the benefits introduced by the multihop aspect of the communications.

The advantages are Packets and a stream cipher encryption mechanism to provide implicit authentication of the nodes involved in the communication. The resulting hybrid ad hoc network also called multi-hop offers several benefits. Reducing the number of antennas is beneficial for the operator because it represents a cost reduction and also because of the NIMBY attitude that makes site acquisition and approval both tedious and difficult. Second the energy consumption of the nodes can be reduced because the signal has to cover a smaller distance. And finally as the radiated energy is reduced the interference with other nodes diminishes as well.

[3] Privacy-preserving routing and incentive protocol called PRIPO for hybrid ad hoc wireless network. PRIPO uses payment to use node cooperation without submitting payment receipts. The lightweight hashing and secret key cryptography operations are implemented to preserve the users privacy. A fixed-size receipt is generated single session regardless of the messages number and only one node has to submit the session receipt instead of submitting it by all the intermediate node. Tp uses statistical tools to identify the cheating nodes by measuring how frequently the nodes reports are inconsistent with others. The solution for this problem are nodes pseudonyms are efficiently computed using hashing operations and Only a trusted party can link these pseudonyms to the real identities for charging and rewarding operations. Propose **PRIPO** a **P**rivacy-Preserving **R**outing and **I**ncentive **P**r**O**tocol for hybrid ad hoc wireless network. PRIPO can foster node cooperation and preserve the privacy of the users locations and communication activities using lightweight hashing and symmetric-key-cryptography operations and without submitting receipts. Extensive evaluations and simulations demonstrate that PRIPO can secure the payment and preserve the users' privacy with acceptable overhead.

[4] Attacks against routing in ad hoc networks to design and performance evaluation of a new secure on demand ad hoc network routing protocol called Ariadne. Ariadne prevent attacker or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes and also prevents many types of Denial-of- Service attacks. Ariadne is efficient using only highly symmetric cryptographic primitives. The main drawbacks are existing infrastructure does not meet application requirements for reasons of security. Researchers in ad hoc networking have generally studied the routing problem in a non-adversarial network setting, in assuming a trusted environment; relatively little research has been done in a more realistic setting in which an adversary may attempt to disrupt the communication. The solutions for this problem are has to give a model for the types of attacks possible in such a system, and the system describe several new attacks on ad hoc network routing

protocols. Second, it present the design and performance evaluation of a new on-demand secure ad hoc network routing protocol, called Ariadne, that withstands node cooperate and relies only on highly efficient *symmetric* cryptography. On-demand routing protocols have been demonstrated to perform better with significantly lower overheads than periodic (or proactive) routing protocols in many situations since the protocol is able to react quickly to the many changes that may occur in node connectivity is able to reduce routing overhead in periods or areas of the network in which changes are less frequent.

[5] The behavior of most mobile system depends heavily on the movement of constituent nodes. Therefore it is highly desirable to have a mobility model that generates stable nodal movement so that the mobile system maintains a steady level of mobility over time, average nodal speed and speed variance. Existing decay provides an unsound basis for simulation studies that collect results averaged over time, complicating the experimental process. The solution for this problem are Analysis that such decay is inevitable in a wide variety of mobility models general framework for describing this decay and apply it to a number of practical cases and this framework allows us to transform any given mobility model into a stationary. Choose initial speeds from the steady-state distribution.

4. System Architecture

Systems design is simply the design of systematic approch. The approach is demanded to the scale and complexity of many systems problems. A systems approach to design is entirely compatible with a user-centered approach. Indeed, the core of both approaches is to understand the users goals. A systems is used to design is most appropriate for projects involving large systems or systems of systems Efficient typically system involve many people from many disciplines working together over an extended period of time. They need tools to deal with their project complexity: defining goals, facilitate communications, and manage processes. The designers working on small projects may find the same tools a bit cumbersome for their needs.

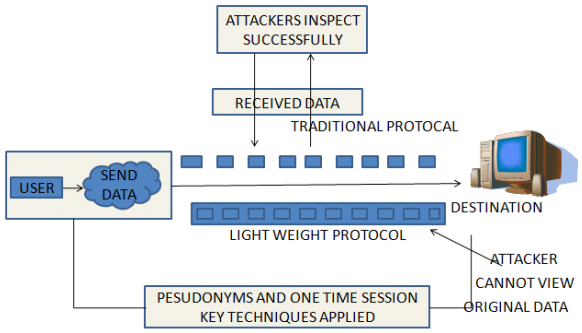

Fig: 1. System Architecture

5. System Module

5.1 Authentication Module

Legitimate users can access the network to prevent unauthorized use. Only legitimate nodes can share keys with base stations and the nodes cannot communicate without these keys. Authenticated packet forwarding: Even though an intermediate node should not know the identity of the other nodes in a route, it should ensure that it relays packets for legitimate nodes to prevent unauthorized use of the network and to ensure that it will be rewarded for relaying packets. In our protocol mutually authenticates the nodes and base stations, and a base station authenticates each node to its neighbors in the route. With these authentications, each node can ensure that it relays packets sent from rightful nodes.

5.2 Secure Data Process Module

Attackers try to correlate the packets sent in one route at different hops by finding information that indicate that the packets belong to the same traffic flow. Communication Security rationality of packet relaying, encourage the nodes' cooperation, and counteract rational cheating actions without the overhead of storing, submitting, and processing receipts. The uplink and downlink intermediate nodes are motivated to relay the data packets because they are rewarded only when the source base station and destination node receive the packets, and thus packet dropping is an irrational action. Relaying DACK packets is beneficial for the downlink nodes because they are rewarded when the packets reach the base station. Privacy Preservation pseudonyms operation changing at each intermediate node guarantee that a packet looks quite different as it is relayed from the source to the destination node called packet content. The packets of a flow can be correlated if they have distinguishable length. Attackers had been find the long time same length node s are transferred with alternative names called packet length.

5.3 Pseudonym Techniques Generation Module

Each pseudonym is used for short time in such a way that only the intended node can link the pseudonyms to each other. The highest privacy level can be obtained when a pseudonym is used for only one packet. Another advantage in our technique is that pseudonyms are computed by lightweight hashing operations and do not require large storage area or pseudonym refilling. Pseudonyms can also be computed before receiving a packet to avoid delaying the packet relay. Pseudonyms are not linkable to the real identity because the real identity is not used in computing them. An attacker cannot link the pseudonyms of a chain without knowing the secret key used in computations and authenticated because no one can compute them except the owner of the secret key.

5.4 Shared Keys authentication and Anonymous Route Module

Each node shares a symmetric key and a pseudonym chain with its cell's base station. Mutually authenticates the node and the base station and distributes shared key to be used in generating pseudonyms. If a node at the same time participates in different routes, it stores each route's pseudonyms and keys in memory, so that it can quickly verify whether a packet is targeted at it or not and which pseudonym/key it has to use. Verification fails, the base station sends a negative acknowledgement to the source node to retransmit the message, and otherwise, it forwards the message to the destination base station if the destination node resides in a different cell. Source node communicate with another node Uplink route between source node's to

base station and Downlink route between the destination node's to base station. To establish end-to-end route, broadcasts the Uplink Route Request Packet and Downlink Route Request Packet to enable to know the identities of the intermediate nodes in the route.

5.5 Accounting and Auditing Module

The base stations can also put into effect access control by rejecting a node's call request if it does not have sufficient credits and complete Accounts. The Data will be reach or receive the base station a data packet, the source and destination nodes are charged and the uplink intermediate nodes are rewarded. The downlink intermediate nodes are rewarded when the destination base station receives acknowledgement for packet delivery.

6. Algorithm Explanation

6.1 Anonymous Pseudonyms and one-time Session Key

The highest privacy level can be obtained when a pseudonym is used for only one packet. Another advantage in our technique is that pseudonyms are computed by lightweight hashing operations and do not require large storage area or pseudonym refilling. Each pseudonym is used for short time in such a way that only the intended node can link the pseudonyms to each other. Pseudonyms are not linkable to the real identity because the real identity is not used in computing them.

6.2 Random Number Generation for Secure Key

Each node shares a symmetric key and a pseudonym chain with its cell's base station. Mutually authenticates the node and the base station and distributes shared key to be used in generating pseudonyms.

7. Conclusion

The pseudonym production technique requires only lightweight hashing operations and does not necessitate large storage area or normally refilling pseudonyms from a trusted party. The pseudonyms are authenticated and can be pre computed to be able to reduce the packet delay and that the proposed protocol can preserve the nodes' privacy with low overhead and secure the payment, route establishment, and data transmission.

Reference

[1] M. Mahmoud, X. Shen, 'ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks, IEEE Trans. on Mobile Computing, 10(7), 2011, 997-1010

[2] M. Mahmoud, X. Shen, Lightweight Privacy-Preserving Routing and Incentive Protocol for HybridAd Hoc Wireless Networks, in Proc. IEEE INFOCOM'11-Int'l Workshop Security Computers, Networking Comm. (SCNC), Shanghai, China, 2011, 1006-1011

[3] Y.-C. Hu, A. Perrig, D. Johnson, Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks, in Proc. ACM Conf. MobiCom Computing and Networking, 2002, 12-23

[4] J. Yoon, M. Liu, B. Nobles, Sound Mobility Models, in Proc. ACM MobiCom, San Diego, CA, USA, 2003, 205-216

[5] Node Cooperation in Hybrid Ad hoc Networks Naouel Ben Salem2, Levente Butty´an3, Jean-Pierre Hubaux2, Markus Jakobsson4, 2005