Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.247 – 249

RESEARCH ARTICLE

Secure Position-Based Routing Protocol for Mobile Ad hoc Networks

S. Sivakumar[1], S. Sagunthala[2]
[1]Department of Computer Science, Periyar University, TamilNadu, India
[2]Department of Computer Science, Periyar University, TamilNadu, India

[1] ssk.pgp@gmail.com; [2] sagupersonal@gmail.com

Abstract— In large and dense mobile ad hoc networks, position-based routing protocols can offer significant performance improvement over topology-based routing protocols by using location information to make forwarding decisions. However, there are several potential security issues for the development of position-based routing protocols. In this paper, we propose a secure geographic forwarding (SGF) mechanism, which provides source authentication, neighbor authentication, and message integrity by using both the shared key and the TIK protocol. By combining SGF with the Grid Location Service (GLS), we propose a Secure Grid Location Service (SGLS) where any receiver can verify the correctness of location messages. We also propose a Local Reputation System (LRS) aiming at detecting and isolating both compromised and selfish users. We present the performance analysis of both SGLS and LRS, and compare them with the original GLS. Simulation results show that SGLS can operate efficiently by using effective cryptographic mechanisms. Results also show that LRS effectively detects and isolates message dropping attackers from the network.

Key Terms: - Ad hoc wireless networks; Location service; Geographic forwarding; Position-based routing protocol; Security

I. INTRODUCTION

Current research on Mobile Ad hoc NET work (MANET) mainly focuses on topology-based routing protocols, including both proactive and reactive (on-demand) approaches [1]. When network topology changes frequently or the network size increases, some of these protocols may incur a significant amount of routing control overhead. Recent research has shown that position-based routing protocols can be good alternatives to topology-based routing protocols in large and dense MANETs [2]. By using Location Information (LI),position-based routing protocols avoid the flooding of control traffic. An intermediate node only needs to know its own position and the positions of its neighboring nodes to make a message forwarding decision. The message is forwarded to a neighbor that is geographically closest to the destination [3–5]. To implement a position-based routing protocol, information about the geographical location of each destination must be available. Each node can determine its own position by using the Global Positioning System (GPS), or its relative position by using GPS free positioning methods [6]. In addition, a location service [7–9] is used by the sender to determine the location of the destination. Each node may have a location table to store the position information of other nodes .In position-based routing; the forwarding decision is based on LI contained in messages. Attackers can alter the LI in messages to disrupt the operation of a unicast forwarding scheme (i.e., message tampering attack). As shown in Fig. 1(a), assume two paths exist between B and A via C (i.e., path BCEA and path BCFDEA). When a node C receives a message m from B, it can modify the LI of A and forward modified message m0 to other colluding node D via node F. When node D receives m0, it will return re-modified message m00 to C

again, and soon. This makes a routing loop where messages traverse nodes in a cycle without being relayed to there all destination A.

II. SECURE GEOGRAPHIC FORWARDING (SGF)

Our proposed secure protocols aim to protect the network layer from attackers. Our proposed schemes work under several assumptions as follows:

1. The network links are bi-directional. That is, if node A is able to transmit to node B, then B is also able to transmit to A.
2. The wireless interface supports promiscuous mode operations. That is, each node can receive a copy of the messages being transmitted by other nodes within its receiving range.
3. All nodes have tightly synchronized clocks with the maximum synchronization error of D.
4. A public key infrastructure exists in the MANET under consideration. Each mobile node stores the trusted certification Authority (CA)'s public key.

We distinguish two main forwarding strategies: greedy forwarding (i.e., unicast) [4] and directional flooding (i.e., broadcast) [5]. In this section, we assume that the source node has already obtained the position information of the destination. The following notations are used in this paper:

1. KTIA ðjÞ [or KTEA ðjÞ] denotes the TIK (or TESLA)key of node A at the j th time interval; KAB denotes the shared secret key between nodes A and B; and KA denotes the private key of node A.
2. MACK(M) denotes the MAC of message M with a symmetric key K using the Hashed MAC algorithm[11].
3. Sign K(M) denotes the digital signature of a message M with the private key K using the public key cryptography [14].

III. SECURE GEOGRAPHIC FORWARDING FOR UNICAST MESSAGES

We propose the use of MAC computed over then on-mutable part (e.g., LI of a destination) of unicast messages with the pair-wise shared secret key between the source and destination. Since intermediate nodes do not have the hared secret key with the source node, they cannot verify the non-mutable part of messages. This allows a compromised ser to be able to modify the non-mutable part of messages to disrupt the operation of position-based routing protocol. To prevent this attack, source node can use the digital signature over the non-mutable part with its own private key n stead of MAC. However, implementing a mechanism to sign the non-mutable parts of all data and control messages may introduce too much overhead. In our scheme, we propose the use of a reputation system (see Section4) to detect and isolate message tampering and drop- ping attackers instead of using expensive digital signatures .We propose to use the TIK protocol [13] with tight time synchronization to authenticate a previous forwarding node to prevent alicious users from joining a path and to avoid a message replay attack. Based on the third assumption stated in each node can estimate the TIK key expiration interval t_{disclosure}. where Mi represents the mutable part of message from sender i, and NS represents the non-mutable part of message from source S. The notation i is equal to S when the sender is a source node itself .The sender i discloses the key K TIi ðjÞ at the end of the same message shows the timelines of sending and receiving a SGF message between two neighbors. Time ti indicates the time when sender starts transmitting the message, and time ti +t_{disclosure} is the disclosure time for key KTIi ðjÞ .Because of the time synchronization, when the neighbor receives the message portion MAC KTIi ðjÞ½MikNSkMACKSD ð N S Þ_, it can verify that the sender i has not started sending the corresponding keyKTIi ðjÞ if the following condition is satisfied :t disclosure g 6 s _ D þ Q=r ð1Þwhere s is the propagation delay, Q is the size of the message excluding K TIi ðj Þ, and r is the transmission rate. As the receiver knows the expiration time for each key and the sender i only discloses the key after it expires, the attackers cannot guess the value of KTIi ðjÞ. Therefore, if the message authentication verifies correctly once the receiver later receives the authentic key KTIi ðjÞ, the message must have originated from the aimed sender. Since only the sender knew the key K TIi ðj Þ, at the time when the receiver received the message, other nodes cannot forge a new message with the correct MAC. Finally, when destination D receives this message, it can verify the authenticity of the message by comparing the received MACKSD ðN SÞ to the MAC value that is computed over the received message NS with the secret key KSD it shares with the source node S. Each node re-establishes its authentic TIK key every th-second with its neighbors by piggybacking on a HELLO message of SGLS. Note that l though there are several forwarding strategies, they all forward a given message to only one optimal neighboring node based on its optimization criterion. Therefore, our proposed SGF can be applied to any of these forwarding schemes without any modification.

IV. LOCAL REPUTATION SYSTEM

Compromised users can disrupt the operation of location services by dropping some control messages, each transmitted in the form of a single unicast message. Moreover, if there is no punishment for misbehaviors, attackers may be rewarded and encouraged to attack again later. In this section, we propose a reputation system with an aim to detect and isolate attackers. We extend the reputation system (i.e., CONFIDENT) originally proposed in [15] and modify it to work specifically for position-based routing protocols. We call our extended version as the Local Reputation System (LRS).Both CONFIDENT and our proposed LRS use the same set of mathematical equations for reputation report update. However, CONFIDENT assumed the use of the source routing protocol. Various ALARM messages are sent to the source node when anomaly is detected. On the other hand, in our proposed LRS, we assume the use of position-based routing protocols. Each node periodically sends the reputation information report to its neighbors by using the HELLO message. In LRS, each node only needs to manage the reputation information of its local neighbors. LRS consists of the following three components: the monitor, the reputation manager, and the trust manager. All these components are present in each node.

V. CONCLUSION

In this paper, we have proposed SGLS, which is a security enhancement to the original GLS protocol .The security mechanisms added to GLS include TIK, TESLA, MAC, digital signature, and a reputation system. SGLS has the capability of preventing message tampering, dropping, falsified injection, and replay attacks. Simulation results showed that in the presence of message dropping attacks, the proposed LRS mechanism maintains a high message delivery ratio at the expense of a higher average end-to-end delay and routing over head in general. For future work, we are planning to implement our algorithm on mobile devices, and study it in real world environments by taking into account the energy issues. Moreover, counter measures against blackmail attacks will be investigated.

REFERENCES

[1] G.G. Finn, Routing and addressing problems in large metropolitan-scale internetworks, Technical Report ISI/ RR-87-180, Inst. for Scientific Information, March 1987.
[2] Z.J. Haas, B. Liang, Ad hoc mobility management with uniform quorum systems, IEEE/ACM Transactions on Networking 7 (2) (1999).
[3] D.B. Johnson, ECC, future resiliency and high security systems, Cert Com White Paper, March 1999.
[4] NS-2 for grid. Available from: <www.pdos.lcs.mit.edu/grid/sim/index.html>.
[5] M. Mauve, J. Widmer, H. Hartenstein, A survey on position based routing in mobile ad hoc networks, IEEE Network 15 (6) (2001) 30–39.

