Location-based Security Authentication Mechanism for Ad hoc Network

Cui Li
School of Computer Science and Software
Tianjin Polytechnic University
Tianjin, China, 15822940409
kdlicui@163.com

Ze Wang
School of Computer Science and Software
Tianjin Polytechnic University
Tianjin, China
bowofran@163.com

***Abstract*—With the growing prevalence of wireless networks, location information plays a critical role in many applications. Especially, in unattended and hostile environment, whether the location of a node lies on a security area became very important. In this paper, we first analyze the security and vulnerability of existing distance estimation techniques. Then utilizing some distance estimation methods, we show a Round-Trip Distance Estimation Algorithm by Verifier Recording Time. Due to its property resisting distance reduction attacks, we provide a location-based security authentication mechanism in ad hoc network. In addition, we show the advantages of our method resisting some common attacks.**

Keywords- Ad hoc networks; location; secure access; distance estimation

I. INTRODUCTION

Research fellows used to study access control mechanisms where one's identity determines what one is authorized to do. However, in practical applications, simple identity information is not enough to protect secure access. For example, in wireless network, sensor nodes are collecting the local information. Once some node deviates from proper environment, i.e. node's location is invalid, the information collected becomes useless. So the physical location of the collector or requester also plays an important role in determining availability of information or access rights. And for most geographical routing protocols, sensor nodes make routing decisions based on their own and their neighbor locations. Recently, many secure localization schemes have been proposed in [1-2]. Those schemes are classified into range-dependent and range-independent localization. In above schemes, researchers assume that locators are trusted and cannot be compromised by an adversary. And Liu et al. proposed a suit of techniques to detect and remove compromised beacon nodes. Respectively speaking, to verify location claims is another technical aspect.

Different from the secure localization mentioned before, this paper focuses on location verification between two nodes by distance estimation. In this paper, our main contributions are summarized as follows. First, we analyze two distance estimation techniques, RF time-of-flight (ToF) and RF distance bounding. And according to prevention methods provided by researchers, we summary the ability of resisting internal attacks and external attacks. Second, based on characteristic of resisting distance reduction attacks for distance estimation methods, we design a novel node-to-node neighborhood authentication mechanism. It helps achieve the desirable goal of localizing the impact of compromise nodes to their vicinity. Finally, we demonstrate how our scheme can act as efficient countermeasures against some notorious attacks.

The rest of this paper is structured as follows. In Section II, we describe some related knowledge. Section III introduces the attacks against distance estimation techniques. In Section IV, we show our technique for location-based security authentication mechanism. Section V and Section VI present our conclusions and acknowledgment respectively.

II. PRELIMINARIES

A. Related Works

Currently, several researchers have put location information as the important factor for security authentication. For example, Liao et al. provided a location-dependent approach for mobile information system. The client can only decrypt the ciphertext when the coordinate acquired form GPS receiver matches with the target coordinate. In 2006, Zhang et al. proposed a location-based key management scheme by binding private keys of individual nodes to both their identities and locations [3].In [4], the IDs of the neighbors instead of the locations as a authenticate factor. [5] analyzed the key compromise impersonation attack of [3] and presented a new location-based authentication scheme. Those methods are very good for resisting some hostile attacks. However, the postulate is that sensor nodes are stationary.

B. Pairing Concept

Let p,q be two large primes and E/F_p indicate an elliptic curve $y^2 = x^3 + ax + b$ over the finite field F_p. We denote by G_1 a q-order subgroup of the additive group of points of E/F_p, and by G_2 a q-order subgroup of the multiplicative group of the finite field $F_{p^2}^*$. The Discrete

Logarithm Problem (DLP) is required to be hard in both G_1 and G_2. For us, a pairing is a map $\hat{e}: G_1 \times G_1 \to G_2$ with the following properties.

1) Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P,Q)^{ab}$, $\forall P, Q \in G_1, \forall a, b \in Z_q$.

2) Non-degeneracy: $\exists P, Q \in G_1$, which are not unit of G_1, then $e(PQ) \neq 1$.

3) Computability: $\exists P, Q \in G_1, e(PQ)$ can be computed efficiently.

III. Attacks Against Distance Estimation Techniques Based on RF

We review some distance estimation techniques and analyze their advantages.

RF ToF-based systems exhibit the better security properties than other techniques. Because RF signals travel at the speed-of-light, an attacker can only increase, but not decrease the measured ToF between the nodes, by jamming and replaying the signals. Of course, if there is an internal attacker, who can cheat on the distance by delaying the signal transmission and reception time. According to different application requests, many people have come up with variant RF TOF distance estimation methods. We summarize the advantages of the distance estimation methods in Table I.

TABLE I. ADVANTAGES OF THE DISTANCE ESTIMATION METHODS

	Resisting internal attackers	Resisting External attackers
Distance bounding	Distance reduction	Distance reduction
Authenticated ranging	NO	Distance reduction
STDEA	NO	Distance reduction and enlargement
RTDEA	NO	Distance reduction and enlargement
K-distance algorithm	Distance reduction	Distance reduction and enlargement

Table I shows that those methods can resist external distance reduction attack. A same reason is that nothing can travel faster than light so that attackers are unable to make the challenge arrive at destination earlier than it should.

STDEA [1], RTDEA [1] can stop the external distance enlargement attack by restraining the time duration (T_{all}) from node sends out the first bit of the response packet until it sends out the last bit of the response packet. $T_{all} > T_a$, $T_a = R/c$ where R is the transmission range of node, and c is the speed of light. To mitigate distance enlargement attack K-distance algorithm [2] requires node to perform K times of distance measurements. By this method, the external attackers might not be able to actively affect all K time measurements. For internal attack, only distance bounding and K-distance algorithm can prevent internal distance reduction attack. The reason is that verifier controls the only timer and converts the time to distance.

IV. Location-based Secure Access Control Mechanism

A. Predeployment Phase

A large-scale ad hoc network consists of hundreds or even thousands of mobile nodes. We assume that all the nodes have the same transmission range R and communicate via bidirectional wireless links. And each node A has a unique, integer-valued and nonzero ID, denoted by ID_A. Because of growing development of positioning technology, many mobile devices can get their position information by themselves. Like GPS, it is today the most widespread outdoor positioning system for mobile devices. So it is assumed that node A has ability to record current location L, denoted by L_A. In view of the cost constraints, nodes are assumed to be not tamper-resistant in the sense that adversaries can extract all the keying material and data stored on a compromised node.

Prior to network deployment, we assume that a trusted authority (TA) does the following operations.

1) Generate the pairing parameters $(p, q, E/F_p, G_1, G_2, \hat{e})$, as described in Section II-A. Select an arbitrary generator W of G_1.

2) Choose two cryptographic hash functions: H, mapping strings to nonzero elements in G_1, and h, mapping arbitrary inputs to fixed-length outputs.

3) Pick a random $k \in Z_q^*$ as the network master secret and set $W_{pub} = kW$.

4) Calculate for each node A an ID-based key (IBK for short), $IK_A = kH(ID_A) \in G_1$.

Each node A is preloaded with the public system parameters $(p, q, E/F_p, G_1, G_2, \hat{e}, H, h, W, W_{pub})$ and its private key IK_A .It is important to note that it is computationally infeasible to deduce k from either (W, W_{pub}) or any (ID, IBK) pair like (ID_A, IK_A), due to the difficulty of solving the DLP in G_1. Therefore, even after compromising an arbitrary number of nodes and their IBKs, adversaries are still unable to calculate the IBKs of noncompromised nodes

B. Location-Based Neighborhood Authentication

In [3], authors proposed the notion of location-based keys (LBKs) by binding private keys of individual nodes to both their IDs and geographic locations. The fact is that LBKs can resist several notorious attacks efficiently, such as the Sybil attack, the identity replication attack, and wormhole and sinkhole attacks. However, WSNs have an intrinsic property that sensor nodes are stationary, i.e., they were fixed at where they were deployed. So this scheme is not suit for mobile networks. To resolve the problem, we provide a new method for mobile network, by using the distance estimation technology.

Neighborhood authentication means the process that any two neighboring nodes validate each other's network membership. This process is fundamental in supporting many security services. For example, a node should only accept messages from and forward messages to authenticated neighbors. Otherwise, external adversaries can easily inject bogus broadcast messages into the network or swindle network secret information from legitimate nodes.

During the post-deployment phase, each node is required to discover and perform mutual authentication with neighboring nodes, which is a normal process in many existing security solutions for wireless networks. In our scheme, each node will consider another node as an authentic neighbor if and only that node is within its transmission range R . We take the following concrete example to explain the neighborhood authentication process. This process is similar to [3].

1) $A \to *: ID_A, L_A, N_A.$

2) $B \to A: ID_B, L_B, N_B, Sig_B(N_A \| N_B \| 1).$

3) $A \to B: Sig_A(N_A \| N_B \| 2).$

Suppose node A wishes to discover and authenticate neighboring nodes. To do so, A locally broadcasts an authentication request including its ID ID_A, location L_A and a random nonce N_A .Upon receipt of such a request, firstly node B needs to ascertain that the claimed location L_A is in its transmission range by verifying if the Euclidean distance $\| L_A - L_B \| \leq R$ This check is the baseline defense against the attack that adversaries surreptitiously tunnel authentication messages between B and a virtually nonneighboring node. Location check is a preliminary test which is that in order to judge the location provided by requester belongs to communication range.

If the inequality does not hold, node B simply discards the authentication request. Otherwise, B estimates the distance to A, by a round-trip distance estimation method. In the method, time is recorded only by verifier (here is B). Then the verifier calculates the last time duration t and distance d_{BA}. So we call it Round-Trip Distance Estimation Algorithm by Verifier Recording Time (VRT-RTDEA). VRT-RTDEA is the similar to the K-Round Distance Estimation Algorithm Zhang et al. proposed. But our algorithm doesn't need to perform K times of distance measurements. Its main purpose is to prevent distance reduction. Because the attacker wants to communicate with benign nodes, only by making the benign nodes believe it belongs to their communication range. The outline of the VRT-RTDEA is shown in Table II.

TABLE II. ROUND-TRIP DISTANCE ESTIMATION ALGORITHM BY VERIFIER TIMING

1: B sends a random challenge nonce m to A.

2: A responds with m and another random nonce n.

3: B sets t = time elapses between challenge and response

4: A sends to B $Sig_A(m \| n)$.

5: **if** $Sig_A(m \| n)$ is right **then** /*by B */

6: $T = (t - t_{tran} - t^A_{proc} - t^B_{proc}) / 2$

7: **end if**

8: **return** $d_{BA} = cT$ /* c is the light speed*/

Firstly, B begins with sending to A random nonce m and starts a timer when the last bit of m is sent. Upon receiving m , node A needs to immediately echo m concatenated by another random nonce n picked by itself. Next, A sends to B $Sig_A(m \| n)$, where $\|$ means message concatenation.

When receiving the last bit of the response, B stops the timer and sets t equal to the elapsing time. It then uses A's public key to compute a MIC on m and n . If the result is not equal to v which arrives later, B considers the response a bogus one and simply ignores it. Otherwise, it believes that the response indeed came from A , and proceeds to calculate the one-way signal propagation time as $T = (t - t_{tran} - t^A_{proc} - t^B_{proc}) / 2$. This procedure displays in Fig.1.

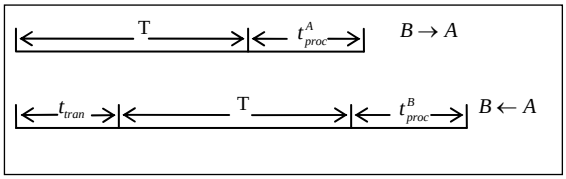

Fig.1. The time plot of the challenge-response process.

Here, t^B_{proc} represents the time duration from when the last bit of the response hits the antenna of A until the response is completely decoded; t^A_{proc} is the time duration from when the last bit of the challenge reaches the antenna

of A until A transmits the first bit of the response. t_{proc}^{B} and t_{proc}^{A} are device-dependent and usually are constant or vary in a tiny scale. Both can be pre-determined and preloaded to B to calibrate the time measurements to certain precision. Assume that transmission links from A to B have a bandwidth of b b/s. Then the response transmission time t_{tran} approximately equal to $2l/b$ seconds.

After verifying $\| L_A - L_B \| \leq R$, B calculates $d_{BA} = cT$ and judges $d_{BA} < R$. If the inequality does not hold, node B ignores the authentication request. Otherwise, B agrees that A is indeed in communication range and a security node. So nodes A and B, B and C can achieve mutual authentication and establish an authentic link between them as shown in Fig.2. Because the distance between A and C do not hold the inequality, node A and C can't establish authentic link.

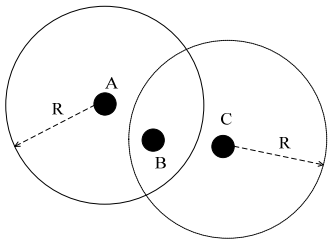

Fig.2. Node-to-node mutual authentication between neighbors.

Function Sig_A and Sig_B are ID-based Signatures. To sign the message M , node B chooses a random $r \in Z_q^*$ and computes:

$$(1)s=\hat{e}(kH(ID_B)W)^r \quad (2)x = h(M \| s) \quad (3)U = (r-x)kH(ID_B)$$

The signature then is the pair $(U,x) \in (G_1, Z_q^*)$. Upon receiving the message M and the signature (U,x) , node A first computes $s' = \hat{e}(U,W)\hat{e}(H(ID_B), W_{pub})^x$, and accepts the signature if and only if $X = h(M \| s')$. The correctness of this scheme is not hard to verify.

C. Security Analysis

This section presents security analysis of our proposed location-based security mechanism. We demonstrate how our mechanism can prevent some malicious attacks.

For example, if an adversary sends an authentication request with a forged location and the location is in node B 's range. In this location forgery attack, it can success though the inequality $\| L_A - L_B \| \leq R$ test, but not reduce the real distance estimation to B . So B gets distance d_{BA} beyond R , that is, inequality $d_{BA} \leq R$ does not hold. Thus this malicious or compromised node cannot pass the screening process by other legitimate nodes. Otherwise, adversaries might as well use the tunneling of authentication messages attack. Over an invisible, out-of-band and low-latency channel, adversaries attempt to make two victim nodes far away from each other believe that they are reasonable authentic neighbors. Because RF signals travel at the speed-of-light, an attacker can only increase, but not decrease the measured ToF between the nodes, by jamming and replaying the signals. So by checking each node will deny authentication requests from nodes that are not physically within its transmission range. About denial-of-service attack, we can set a threshold value for the number of malicious nodes checked out by a benign node. Once the number is more than the threshold value, it indicates existing DoS attack. As for clone attack, there are some typical methods resisting it. A solution that prevents this attack is to nodes tamper-proof such that attacker do not see their authentication material and cannot clone them. Another method is that nodes perform device fingerprinting by which they identify each device as unique. In that case, the nodes can identify a device by the unique "fingerprint" that characterizes its signal transmission.

So in mobile ad hoc network, our authentication mechanism is effective for preventing those common attacks.

V. CONCLUSION

In this paper, we analyze the special superiorities of the different distance estimation techniques. Then we show a Round-Trip Distance Estimation Algorithm by Verifier Recording Time (VRT-RTDEA). Taking advantage of VRT-RTDEA's property resisting distance reduction attacks, we provide a location-based security authentication mechanism for ad hoc network. And we demonstrate some malicious attacks cannot be launched. In fact, Our authentication is not only suit for mobile network, but also static network. In the future research, we plan to expend and perfect mechanism security. We also intend to further investigate the potentials of location-based verification for dynamic network.

REFERENCES

[1] Daojing He, Lin Cui, Hejiao Huang. "Design and verification of enhanced secure localization scheme in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, VOL. 20, NO. 7, pp.1050–1058,2009.

[2] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure Localization and Authentication in Ultra-Wideband Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 4, pp. 829-835, Apr. 2006.

[3] Y. Zhang, W. Liu, Y. Fang. Location-based compromise-tolerant security mechanisms for wireless sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24 (2):247–260.

[4] K. Xue, W. Xiong, P. Hong, H. Lu, NBK: A novel neighborhood based key distribution scheme for wireless sensor networks, International Conference on Networking and Services, 2009, pp. 175–179.

[5] M.J.Duan , J.Xu, An Efficient Location-based Compromise-tolerant Key Manament Scheme for Sensor Networks [J], Information Processing Letters,2011,111(11):503-507.