Design and Verification of Enhanced Secure Localization Scheme in Wireless Sensor Networks

Daojing He, Lin Cui, Hejiao Huang, *Member*, *IEEE*, and Maode Ma, *Member*, *IEEE*

Abstract—In this paper, we focus on the need for secure and efficient localization for wireless sensor networks in adversarial settings. An attack-resistant and efficient localization scheme is developed, which extends the scheme proposed in [1]. The method offers strong defense against not only distance reduction attacks but also distance enlargement attacks. Furthermore, our method does not employ any device-dependent variables, hence yields more accurate localization. An attack-driven model is also specified using Petri net. It provides a formal method for the verification of our scheme when considering distance enlargement attacks. The state analysis shows that the potential insecure states are unreachable, implying that the model can offer strong defense against these attacks. To the best of our knowledge, it is the first time that the Petri net has been introduced to validate security scheme for wireless sensor networks in the literature.

Index Terms—Localization, security, wireless sensor networks.

1 Introduction

In wireless sensor networks (WSNs), sensor locations play a critical role in many applications. Not only do applications such as environment monitoring and target tracking require sensor locations to accomplish their tasks, but several fundamental techniques in WSNs also require sensor locations. For example, in most geographical routing protocols (e.g., GPSR [2]), sensor nodes make routing decisions at least partially based on their own and their neighbor locations. However, due to the cost reasons, it is not practical to equip a GPS receiver on every sensor node. Driven by this demand, many localization schemes have been proposed to reduce or completely remove the dependence on GPS in WSNs [3], [4], [5], [6], [7], [8], [9], [10], [11]. All of these methods assume the existence of a few anchor nodes [i.e., beacon nodes (BNs)] knowing their own locations (e.g., through GPS receivers or manual configuration).

The above proposed techniques were mainly studied in trusted environment. However, WSNs may be deployed in hostile environments, and localization may become the target of attacks due to its importance. Because of the threats to WSN localization in a hostile environment, the development of secure localization algorithms is mandated. Further, due to the resource constraints of a typical sensor node, the secure localization algorithm has to be efficient in terms of computation and memory requirement.

Recently, a number of secure localization schemes (SLSs) have been proposed [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23]. These techniques rely on robust statistics, directional antennas, or spread spectrum techniques using spreading codes, and so on. Basically, these methods can be categorized into four kinds as follows:

One way to deal with malicious nodes is to accept that they will be present in the network and propose robust position computations that are still able to work in the presence of bogus information. This is accomplished mostly by using statistical and outlier filtering techniques. In these cases, it is assumed that benign nodes outnumber malicious ones. For example, the Attack-Resistant Minimum Mean Square Estimation (ARMMSE) [14] is a voting-based location estimation working based on the observation that a location reference that has been attacked is usually much different from benign ones, since it can mislead location estimation. Thus, ARMMSE uses the "inconsistency" among the location references provided by anchors to identify the malicious injection and discard them before making a final location estimation. This scheme has each location reference vote on the locations at which the node may reside on a grid of cells. Then, the cell(s) with the highest vote will be selected and the center of the cell(s) will be considered as the estimated location. Li et al. [15] studied and developed an attack resilient location estimator based on Least Median of Squares (LMS). The idea is to draw random subsets of data from the original data pool for individual subset estimation and then combine these estimations based on estimation quality. Wang et al. [16] suggested the cluster-based minimum mean square estimation (CMMSE) algorithm, which was the fastest scheme among all the ones evaluated. All of these methods have

- *D. He, L. Cui, and H. Huang are with the Department of Computer Science, Harbin Institute of Technology Shenzhen Graduate School, HIT Campus Shenzhen University Town Xili, Shenzhen, Guangdong 518055, P.R. China. E-mail: {hedaojinghit, cuilincui}@gmail.com, hjhuang@hitsz.edu.cn.*
- *M. Ma is with the School of Electrical and Electronic Engineering, Division of Communication Engineering, Nanyang Technological University, Nanyang Avenue, Singapore 639798. E-mail: emdma@ntu.edu.sg.*

Manuscript received 11 Feb. 2008; revised 19 Aug. 2008; accepted 21 Aug. 2008; published online 27 Aug. 2008.
Recommended for acceptance by K. Hwang.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2008-02-0054.
Digital Object Identifier no. 10.1109/TPDS.2008.166.

mitigated the attacks with two disadvantages. First, they all focus on the statistical analysis of the results without the process of the measurement leading them potentially insecure. Second, all of these methods are based on the assumption that most of the measurements will not be attacked, which is not true in real world.

Another kind of security method is to observe the behavior of nodes and decide whether to trust them. Liu et al. [17] propose a suite of techniques to detect and remove compromised BNs. One technique is that the detecting node compares the calculated distance by using the location information provided by the target node and the estimated distance by means of the signal (e.g., RSSI). Another technique to filter out locally replayed beacon signals is based on the observation that the replay of a beacon signal introduces extra delay. In most cases, this delay is large enough to detect whether there is a locally replayed beacon signal through the round-trip time (RTT) between two neighbor nodes. Srinivasan et al. [18] propose a novel reputation-based scheme called Distributed Reputation-based Beacon Trust System (DRBTS) for excluding malicious BNs that provide false location information. In DRBTS, every BN monitors its one-hop neighborhood for misbehaving BNs and provides information by maintaining and exchanging a neighbor reputation. However, these methods just focus on the security of anchor. Moreover, they need more computation and energy resource.

Also, some other methods focus on the validation of the final position estimation rather than avoiding or detecting compromised nodes and attacks. Localization anomaly detection (LAD) [19] uses deployment knowledge, with a group-based deployment model, to let sensors verify whether their derived locations are consistent with the known deployment knowledge. In [20], an algorithm is proposed for in-region verification in which a set of nodes wishes to verify whether another node is inside the particular region. This particular region may be a room, a building, or other physical area. The proposed protocol, called Echo, uses known physical properties of both radio frequency and ultrasound to compute distances and check whether a node really can be inside the claimed region. These methods require deployment knowledge or physical properties of both radio frequency and ultrasound. Thus, their application is restricted. Moreover, they are not very precise.

There are several other secure localization techniques including SeRLoc [21], SPINE [22], and ROPE [23]. However, SeRLoc requires directional antenna on sensor nodes. SPINE requires nanosecond scale time synchronization among all sensor nodes. ROPE, which is an integration of SeRLoc and SPINE, requires both directional antenna and nanosecond scale time synchronization. These requirements cannot be met on the current generation of sensor platforms such as MICA series.

In connection, Zhang et al. [1] analyzed and enhanced the security of existing approaches when applied in adversarial settings and then presented a novel mobility-assisted SLS. The anchor A at time t_1 transmits a challenge to sensor S, which immediately echoes a response received by A at time t_2. Anchor A can then estimate its distance to S as $(t_2 - t_1 - T)c/2$, where c is the speed of light, and T is a device-dependent variable, which is set to be a constant value in this scheme. Compared with the distance reduction attacks, distance enlargement attacks are more complicated, which enlarge $(t_2 - t_1)$, thus the distance estimate. To mitigate the attacks, anchors repeat the process above for K times and take the median of the K distance estimates. Because of the potential distance enlargement attacks, there is a distance validity test in the end.

Although the SLS above offered strong defense against distance reduction attack, it only can mitigate distance enlargement attack through a series of steps such as taking median of K distance estimates and validity test. And, it can only tolerate at most 50 percent attacked enlargement measurements. Furthermore, the distance computing of the SLS presented in [1] depends on three kinds of time durations, which are all device dependent. Although those time durations are claimed to be usually constant or vary in a tiny scale, they may lead to inaccurate localization.

To develop a more secure and efficient localization scheme and avoid the problems of the above approaches, we propose an Enhanced SLS (ESLS) in this paper. It extends the method in [1]. There are two approaches according to whether there is a synchronous timer among anchors and the other nodes. The ESLS can be specified based on Petri net model and the attacks can be verified efficiently. To the best of our knowledge, it is the first time that the Petri net has been introduced to validate security scheme for WSNs in the literature.

The rest of this paper is organized as follows: In Section 2, we first present an ESLS with two algorithms. Then, in Section 3, an attack-driven model using Petri net and a formal method for verification of our scheme under distance enlargement attacks are given. Finally, our work is summarized in Section 4.

2 Enhanced Secure Localization Scheme

In this section, we present an ESLS for WSNs. To ease our illustration, we focus on the 2D location estimation, but the ESLS can be easily extended to the 3D case.

2.1 Vulnerability Analysis of Two-Way Time-of-Arrival (ToA) Localization

Time of arrival (ToA) is one of the most commonly used localization technique whose requirement for fine time resolution can be satisfied in many scenarios (for example, UWB technique). In this paper, we only focus on the two-way ToA approach (Fig. 1).

In the shown example, we assume A, B, and C know its own position as (X_A, Y_A), (X_B, Y_B), and (X_C, Y_C). A transmits at time t_1 a challenge to sensor S, which immediately echoes a response received by A at time t_2. Then, estimated distance between A and S is $d_{AS} \approx (t_2 - t_1)c/2$, where c is the speed of light. In the same way, the distance to S from B and C can be obtained, say d_{BS} and d_{CS}, respectively. Suppose that A is the leader that collects d_{BS} and d_{CS} and then obtains S's location by the following equations:

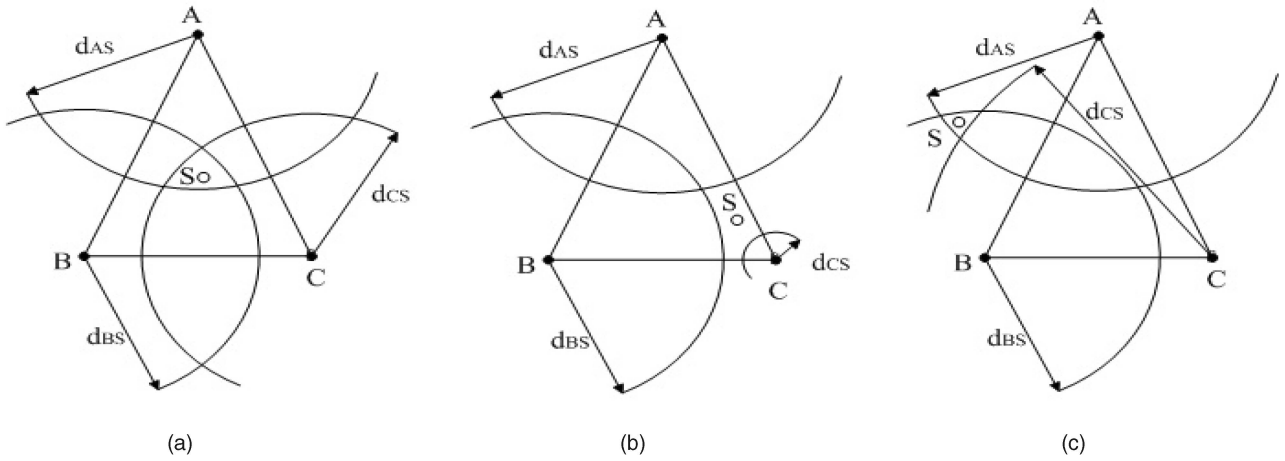

Fig. 1. An exemplary two-way ToA localization process, where anchors A, B, and C determine the localization of sensor S. (a) No attacks. (b) d_{CS} is reduced. (c) d_{CS} is enlarged.

$$\begin{cases} f_A = d_{AS} - \sqrt{(X_S - X_A)^2 + (Y_S - Y_A)^2}, \\ f_B = d_{BS} - \sqrt{(X_S - X_B)^2 + (Y_S - Y_B)^2}, \\ f_C = d_{CS} - \sqrt{(X_S - X_C)^2 + (Y_S - Y_C)^2}, \end{cases} \quad (1)$$

where f_A, f_B, and f_C are all supposed to be zero when no error occurred during the above process. Because measurement errors inevitably exist in reality, (X_S, Y_S) will be somewhere in the intersection area formed by the three circles, as shown in Fig. 1a. By deriving the minimum mean-square error (MMSE) location estimation [24], we can obtain a more precious estimation.

The above process is vulnerable to distance reduction (Fig. 1b) and enlargement attacks (Fig. 1c), which maliciously increase the location inaccuracy. For example, attackers may answer anchor C's challenge in the name of S while jamming the later genuine response from S to reduce d_{CS}. In addition, an example of distance enlargement attack is shown in Fig. 2, where the two circles indicate the transmission ranges of anchor C and attacker 2, respectively. The challenge from C is correctly received by attacker 1 but not by sensor S, which is jammed by attacker 2. Then, this challenge will be sent to attacker 2 through a secret channel, and attacker 2 forwards the challenge to sensor S after some time. Because the challenge is not modified by attackers, sensor S will consider it a challenge from anchor C and respond to it, and thus the distance estimate is increased.

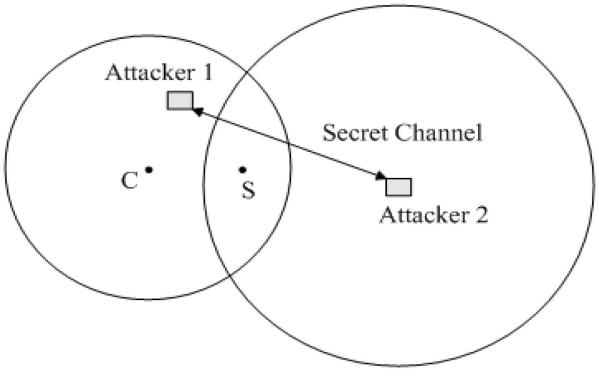

Fig. 2. Topology of an exemplary distance enlargement attack.

2.2 Network Model

Our network model is similar to the model described in [1]. The detailed description is given as follows:

We consider a WSN that consists of randomly deployed sensor nodes, e.g., via random aerial scattering. Sensor localization is normally done during the network initialization phase, in which we assume that a set of anchors, denoted by α, performs coordinated group movement across the whole sensor field. Typical examples of anchors are mobile robots or unmanned aerial vehicles (UAVs) flying at low levels. The number of anchors, denoted by $N_a = |\alpha|$, should be at least three to determine a 2D location. Intuitively, the more anchors (i.e., distance estimates) are available, the more precise location estimations are at the cost of increased communication and computational overhead. We also indicate anchor i by A_i for $i = \{1, \ldots, N_a\}$.

Each A_i is assumed to know its own location (X_{A_i}, Y_{A_i}) at any time and place through GPS receivers. In addition, there is always a leader in α that takes charge of the localization process. In practice, each anchor should take turns to act as the leader to balance their resource usage. For convenience, however, we assume A_1 to be always the anchor leader hereafter. We further assume that anchors and sensor nodes have the same transmission range r_0.

Before network deployment, we assume that the network planner picks a sufficiently long secret κ and loads each sensor S with a secret key $\mathrm{K}_S = h_\kappa(ID_S)$. Here, ID_S is the unique identifier of node S, h indicates a fast hash function such as SHA-1, and $h_\kappa(M)$ refers to the message integrity code (MIC) of message M under key κ. We further postulate that each anchor knows the network secret κ and is trusted and unassailable to attackers during the node localization phase, which usually does not last too long. This assumption is reasonable in that anchors are usually much fewer than sensor nodes. Moreover, some researchers [17], [18] have proposed some techniques to detect compromised anchor nodes with localization information. And, this is beyond our present scope.

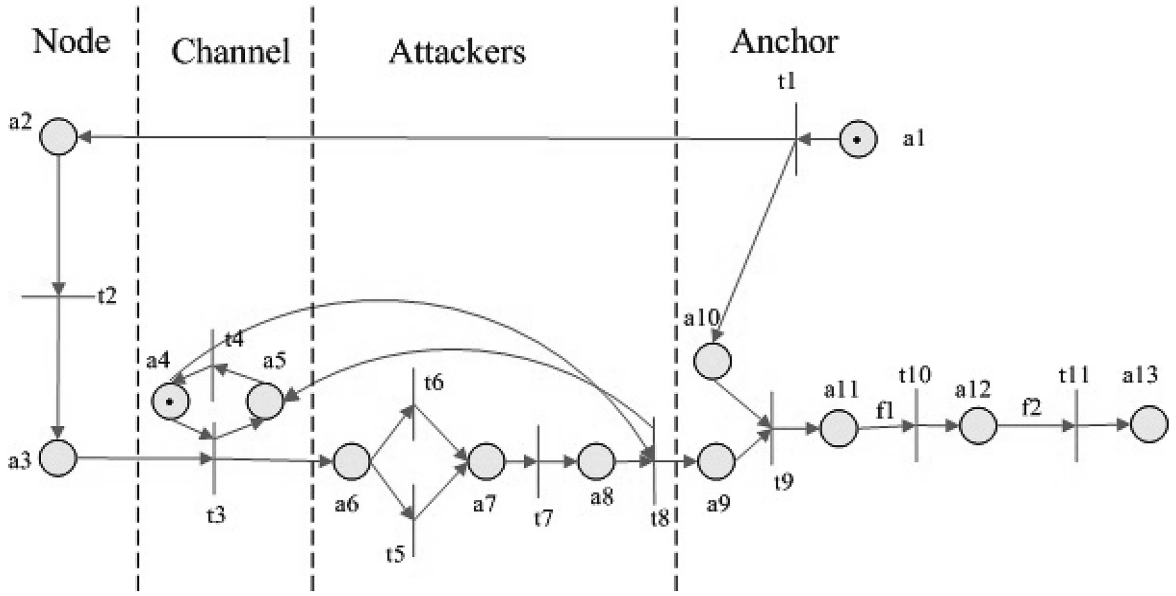

Fig. 3. Petri net model for the STDEA shown in Table 1 under attacks.

2.3 Overview of ESLS

After sensor nodes are deployed, anchors are instructed to perform strategic group movement along preplanned routes to localize all the sensor nodes. Anchors are required to always maintain an N_a-vertex polygon with the longest distance between any two vertices no larger than r_0. This means that anchors and sensors inside the polygon can directly communicate with each other. To localize a node, say S, anchors first measure their respective distance to S with a novel two-trip ToA approach. The anchor leader then collects all the distance estimations whereby an MMSE location estimation is derived [24]. Subsequently, A_1 runs a validity test on the location estimate to detect possible attacks.

In the rest of this section, we will detail the operations of this ESLS with an example. We focus on getting the distance between anchor A_i and node S securely and efficiently.

2.4 Two Kinds of Distance Estimation Algorithms

There are two distance estimation algorithms according to whether it requires time synchronization among all the anchors and nodes.

2.4.1 Single Trip Distance Estimation Algorithm

The Single-Trip Distance Estimation Algorithm (STDEA) requires time synchronization among all the anchors and nodes (Fig. 3).

Let T_{all} denote the time duration from the moment node S sends out the first bit of the response packet until it sends out the last bit of the response packet. To defend against the distance enlargement attack, we only require $T_{all} > T_a$, where $T_a = \frac{r_0}{c}$, and c is the speed of light.

To obtain a distance estimate to node S, anchor A_i first calculates $\mathrm{K}_S = h_\kappa(ID_S)$ based on the preloaded network secret κ. It then executes the STDEA outlined in Table 1.

The process of the STDEA is given as follows:

A_i begins with sending to S an l-bit random nonce m. Upon receiving m, node S needs to echo one packet. The response packet consists of m, T_1, and MIC $a = h_{\kappa_S}(m \| T_1)$, where T_1 is the time when S sends the first bit of the response packet. A_i receives the response and sets T_2 = the time when it receives the first bit of the response packet. And, A_i then uses K_S to compute MIC on m and T_1. If the result is not equal to a, A_i considers the response a bogus one and simply ignores this packet from S. Then, A_i checks the value of $|T_2 - T_1|$. If $|T_2 - T_1| > T_a$, the packet must be delayed by attackers and A_i simply ignores this packet from S. If $|T_2 - T_1| \leq T_a$ and the MIC is correct, A_i believes that the response indeed came from S and proceeds to calculate the single-trip signal propagation time as $t = T_2 - T_1$, and the estimate distance between A_i and S is ct. Thus, there are two cases in which A_i considers the response a bogus one and simply ignores the packet from S.

The above process of the STDEA offers strong defense against not only distance reduction attacks but also distance enlargement attacks. And, the distance computing between S and A_i is simple, which is not related to the device-dependent time as the SLS. A more detailed analysis is given as follows:

Our method offers strong defense against distance reduction attacks in the sense that attackers are not able to reduce t and, thus, the distance estimate ct (c denotes the speed of light). Because of the synchronous timer we introduced, the attackers have to reduce the time duration of the response packet sent from S to A_i in order to reduce the distance estimate. However, nothing can travel faster than light so that attackers cannot make the response packet arrive at A_i earlier than it should. Furthermore, our method also offers strong defense against distance enlargement attacks. Since there is only a single shared wireless channel, there is only one way to launch distance enlargement attacks. Otherwise, there would be collisions at anchor A_i. The sole mean is that the attackers have to spend at least T_a time to receive the whole packet sent by S and then forward it to A_i. Thus, in distance enlargement attacks, the value of $|T_2 - T_1|$ would be larger than T_a, which can be detected by A_i.

TABLE 1
STDEA

1:	A_i sends a random challenge nonce m to S
2:	S responds a packet to A_i with m, T_1, and $a = h_{\kappa_S}(m \| T_1)$, where T_1 = the time when S sends the first bit of the response packet
3:	A_i receives the response and sets T_2 = the time when A_i receives the first bit of the response packet
4:	if $h_{\kappa_S}(m \| T_1) == a$ then /*by A_i */
5:	if $\lvert T_2 - T_1 \rvert > T_a$ then
6:	return error
7:	end if
8:	$t = T_2 - T_1$
9:	return $d_{A_iS} = ct$ /* c is the speed-of-light */
10:	else
11:	return error
12:	end if

Note that the attacker can either be an insider or an outsider [12], [13]. As an insider, the attacker has access to all of the cryptographic keying material held by a node. It is potentially dangerous that the attacker can claim to be a legitimate part of the network. On the other hand, as an outsider, the attacker can only capture a node but cannot extract the sensitive information. This model is comparatively less detrimental but harmful nonetheless. So, for a localization process to be secure, it has to be robust in its defense against both outside and inside attacks. Our model has a focus on preventing the outside attacks.

2.4.2 Round-Trip Distance Estimation Algorithm

The STDEA requires time synchronization among all the anchors and nodes before deployment. In order to relieve this requirement on the devices, we consider a method that does not rely on time synchronization among all the anchors and nodes, that is, the Round-Trip Distance Estimation Algorithm (RTDEA).

RTDEA is the similar to the previous work of the STDEA but with a synchronous timer. The outline of the RTDEA is shown in Table 2.

The key idea of RTDEA is similar to STDEA. The process of RTDEA is given as follows:

A_i sends a request packet to S. The packet consists of a random nonce m, T_1, and $a = h_{\kappa_S}(m \| T_1)$, where T_1 is the time when A_i sends the first bit of the request packet. S receives the packet and checks the MIC. If the packet is valid, S will send a response packet with m, T_2, T_3, another random nonce e, and $a = h_{\kappa_S}(m \| e \| T_2 \| T_3)$ to A_i. Then, A_i receives the response packet and sets T_4 = the time when it receives the first bit of the response sent by S. And, A_i then uses K_S to compute an MIC on m, e, T_2, and T_3. If the result does not equal to a, A_i considers the response a bogus one and simply ignores the packet from S. Then, A_i checks the value of $|T_4 - T_1 - (T_3 - T_2)|$. If $|T_4 - T_1 - (T_3 - T_2)| > 2T_a$, the packet must be delayed by attackers and A_i simply ignores this packet from S. If $|T_4 - T_1 - (T_3 - T_2)| \leq 2T_a$ and the MIC is correct, A_i believes that the response indeed came from S and proceeds to calculate the single-trip signal propagation time as $t = (T_4 - T_1 - (T_3 - T_2))/2$, and the estimate distance between A_i and S is ct (c denote the speed of light).

Let TA_{all} denote the time duration from the moment anchor A_i sends the first bit of the request packet until it sends the last bit of the request packet, and TS_{all} denote the time duration from the moment node S sends the first bit of the response packet until it sends the last bit of the response packet. To defend against the distance enlargement attack, we only require $TA_{all} > 2T_a$ and $TS_{all} > 2T_a$, where $T_a = \frac{r_0}{c}$, and c is the speed of light.

Attack analysis for the RTDEA is similar to the STDEA, as mentioned in Section 2.3.1. Here, we only focus on the distance enlargement attack. Since there is only a single shared wireless channel, there are only two means to launch distance enlargement attack. Otherwise, there would be collisions at either anchor A_i or node S. The two means are given as follows: One is that the attackers have to spend at least $2T_a$ time to receive the whole request packet sent by A_i and then forward it to node S. The other is that they have to spend at least $2T_a$ time to receive the whole response packet sent by S and then forward it to anchor A_i. Thus, in distance enlargement attack, the value of $|T4 - T1 - (T3 - T2)|$ would be larger than $2T_a$, which can be detected by anchor A_i. Thus, we can obtain that the RTDEA offers strong defense against not only distance reduction attacks but also distance enlargement attacks.

3 Attack-Driven Model and Verification

Petri net is a graphical and mathematical tool applicable to model many complex systems. It is a tool for describing and studying systems that are characterized as being concurrent, asynchronous, distributed, parallel, and/or nondeterministic. It can be used to set up state equations, algebraic equations, and other mathematical models for describing the behavior of systems. Petri net is also applicable for verifying the security problems under the environment

TABLE 2
RTDEA

1: A_i sends a request packet to S with a random nonce m, T_1 and $a = h_{\kappa_S}(m \| T_1)$, where T_1 is the time when A_i sends the first bit of the packet
2: S receives the packet and sets T_2 = the time when it receives the first bit of the packet sent by A_i
3: if $h_{\kappa_S}(m \| T_1) == a$ then /*by S */
4: S sends a response packet to A_i with m, T_2, T_3, another random nonce e and $a = h_{\kappa_S}(m \| e \| T_2 \| T_3)$, where T_3 = the time when S sends the first bit of the response packet to A_i
5: A_i receives the response sent by S, and sets T_4 = the time when it receives the first bit of the response packet sent by S
6: if $h_{\kappa_S}(m \| e \| T_2 \| T_3) == a$ then /*by A_i */
7: if $|T_4 - T_1 - (T_3 - T_2)| > 2T_a$ then
8: return error
9: end if
10: $t = (T_4 - T_1 - (T_3 - T_2))/2$
11: return $d_{A_i S} = ct$ /* c is the speed of light*/
12: else
13: return error
14: end if
15: else
16: return error
17: end if

with attackers (e.g., [25]). The formal definition of Petri nets and the incidence matrix are given as follows: For more information about Petri nets, the reader is referred to [26].

A Petri net is a five-tuple $N = (P, T, F, W, M_0)$, where

1. P is a finite set of *places*;
2. T is a finite set of *transitions* such that $P \cap T = \emptyset$ and $P \cup T \neq \emptyset$;
3. $F \subseteq (P \times T) \cup (T \times P)$ is the *flow relation*;
4. W is a weight function such that $W(x, y) \in \mathrm{N}^+$ (positive integers) if $(x, y) \in F$ and $W(x, y) = 0$ if $(x, y) \notin F$; and
5. M_0 is an initial state of the system.

Pictorially, a Petri net is a bipartite directed graph with two kinds of nodes: P represented with cycles and T represented with boxes. The arcs in F connect P and T, and a weight value in W is assigned to each arc. Initially, there are some tokens, represented with blacks dots, distributed in some places representing the initial marking. A transition may fire when it is enabled, which means that there are enough tokens at the end of all input arcs. When the transition fires, it consumes these tokens and places some appointed number of tokens at the end of all output arcs.

The incidence matrix V of a net N is a $|P| \times |T|$ matrix whose element v_{ij} at row p_i and column t_j is calculated by $v_{ij} = W(t_j, p_i) - W(p_i, t_j)$.

Usually, in a Petri net model, places are used to model state while transitions are used to specify operations or actions.

In this section, based on Petri net, we will develop an attack-driven model for STDEA and apply a formal method for the verification of distance enlargement attacks. The model can also be easily extended for the RTDEA.

3.1 Petri Net Modeling for Attack-Driven Scheme

As shown in Fig. 1, we develop a Petri net for the whole process of the STDEA as mentioned in Table 1 under attacks. We just consider the cases which attackers modify or delay the exchanged packets. There are four areas corresponding to node, channel, attackers, and anchor, respectively. The model can be easily extended to the RTDEA.

The default weight of each arc is 1 except the one that is marked. And, the definition of f1 and f2 are given as follows:

$$\mathrm{f1} = 2^{|H_{K_S}(m \| T_1) - a|},$$

$$\mathrm{f2} = g(T_a - (T_2 - T_1)), \quad g(x) = \begin{cases} 1, & x \geq 0, \\ 2, & x < 0. \end{cases}$$

Table 3 lists the specification of each place in Fig. 1, and Table 4 lists the specification of each transition in Fig. 1.

In the initial state, there is one token in places a1 and a4, respectively. The token in a1 is used to start the localization request for anchor. And, the other one in a4 is functioned as a shared channel between the anchor and the node.

TABLE 3
Specification of Each Place in Fig. 1

Name	Definition
a1	A request for localization sent by anchor
a2	node receives the request packet sent by anchor
a3	node sends out the response packet
a4,a5	channel
a6	attacket1 receives the packet
a7	attacker1 has stored or tampered the packet
a8	attacker2 receives a packet from attacker1
a9	anchor receives a packet
a10	anchor is ready to receive packets
a11	anchor has received the packet
a12	anchor has checked the MIC of the packet
a13	anchor checks $\lvert T_2 - T_1 \rvert$ is ok

TABLE 4
Specification of Each Transition in Fig. 1

t1	Anchor sends a request
t2	node sends the response packet, with m, T_1, and MIC
t4,t5,t9	channel operations
t6	attacker1 stores the packet
t7	attacket1 tampers the packet
t8	attacker1 sends a packet to attacker2
t9	anchor receives the response packet and records the time when it receives the first bit of the response packet (T_2)
t10	anchor checks the MIC of the packet
t11	anchor checks $\lvert T_2 - T_1 \rvert$

Transitions t10 and t11 represent the validation implemented by the anchor. Thus, a successful localization process is that both t10 and t11 are fired and there is a token in a13. In the other case, there may be attacks during the process.

3.2 Verification of the Security Based on Petri Net Model

The state equation technique is usually applied for the verification of a reachable marking in Petri net theory. And, the state equation is

$$M_n = M_0 + C^T\sigma, \tag{2}$$

where σ is the count of the transition sequence from M_0 to M_n.

If the state M_n is reachable from M_0, the state equation should be satisfied. In other words, if there are no solutions for the equation, the final state M_n would be unreachable. So, we can use the state equation to determine whether an acceptable state is reachable when there are attacks.

In Fig. 1, the acceptable state M_n of our model is (a1, a2, a3 ... a13), where all the values are 0 except that each of a4 and a13 is 1.

The initial state M_0 is (a1, a2, a3 ... a13), where all the values are 0 except that both a1 and a4 are equal to 1. Table 5 lists the incidence matrix.

The analysis is given as follows:

If attackers tamper with the packet, the value of f1 in C^T would be larger than 1. For nonhomogenous equations, if the rank of the coefficient matrix is less than the rank of the augmented matrix, the equations has no solution. Thus, we can obtain that the state equation has no solution if f1 $>$ 1.

TABLE 5
Incidence Matrix

	t1	t2	t3	t4	t5	t6	t7	t8	t9	t10	t11
a1	-1										
a2	1	-1									
a3		1	-1								
a4			-1	1				-1			
a5			1	-1				1			
a6			1		-1	-1					
a7					1	1	-1				
a8							1	-1			
a9								1	-1		
a10	1								-1		
a11									1	-f1	
a12										1	-f2
a13											1

That means the acceptable state is unreachable when attackers tampered the packet.

If collusion attackers delay the packet, $|T_2 - T_1|$ in C^T would be larger than T_a, then $\mathrm{f2} = 2$, the state equation also has no solution, and the acceptable state is unreachable.

So, if there are any distance enlargement attacks, our model will not reach the acceptable state. In other words, our model offers strong defense against these attacks.

4 Conclusion and Future Work

In this paper, we have proposed a reliable mechanism called ESLS to enhance the functions of the SLS in [1]. Our method offers strong defense against not only distance reduction attacks, but also distance enlargement attacks. Furthermore, it is a device-independent scheme with strong function of more accurate localization. An attack-driven model has also been developed by using Petri net. It provides a formal method for the verification of our scheme considering distance enlargement attacks. The state analysis shows that the potential insecure states are unreachable, implying that the model can offer strong defense against these attacks. Our algorithms make no assumptions on the underlying network and therefore are applicable to a wide range of wireless network settings including wireless ad hoc networks, WSNs, wireless mesh networks, and so forth. In our future work, we plan to use some extended Petri net (for example, colored and time Petri net) to give a more powerful verification of our scheme. The introduction of our method into multichannel wireless networks would be another future work.

Acknowledgments

The work reported in this article was financially supported by National Natural Science Foundation of China under Grant No. 10701030, National High-Tech R&D program (863 Program) under Grant No. 2006AA01Z197, and in part by the National Basic Research Program of China (973 Program) under Grant No. 2006CB303000.

References

[1] 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.

[2] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," *Proc. ACM MobiCom*, 2000.

[3] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-Less Low Cost Outdoor Localization for Very Small Devices," *IEEE Personal Comm. Magazine*, pp. 28-34, Oct. 2000.

[4] A. Savvides, C. Han, and M. Srivastava, "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," *Proc. ACM MobiCom '01* pp. 166-179, July 2001.

[5] L. Doherty, K.S. Pister, and L.E. Ghaoui, "Convex Optimization Methods for Sensor Node Position Estimation," *Proc. IEEE INFOCOM*, 2001.

[6] A. Nasipuri and K. Li, "A Directionality Based Location Discovery Scheme for Wireless Sensor Networks," *Proc. ACM Int'l Workshop Wireless Sensor Networks and Applications (WSNA '02)*, Sept. 2002.

[7] A. Savvides, H. Park, and M. Srivastava, "The Bits and Flops of the N-Hop Multilateration Primitive for Node Localization Problems," *Proc. ACM Int'l Workshop Wireless Sensor Networks and Applications (WSNA '02)*, Sept. 2002.

[8] T. He, C. Huang, B.M. Blum, J.A. Stankovic, and T.F. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Networks," *Proc. ACM MobiCom*, 2003.

[9] R. Nagpal, H. Shrobe, and J. Bachrach, "Organizing a Global Coordinate System from Local Information on an Ad Hoc Sensor Network," *Proc. Second Int'l Workshop Information Processing in Sensor Networks (IPSN)*, 2003.

[10] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) Using AoA," *Proc. IEEE INFOCOM '03*, pp. 1734-1743, Apr. 2003.

[11] D. Niculescu and B. Nath, "DV Based Positioning in Ad Hoc Network," *J. Telecomm. Systems*, 2003.

[12] A. Srinivasan and J. Wu, "A Survey on Secure Localization in Wireless Sensor Networks," *Encyclopedia of Wireless and Mobile Comm.*, CRC Press, Taylor and Francis Group, 2007.

[13] A. Boukerche, H.A.B. Oliveira, E.F. Nakamura, and A.A.F. Loureiro, "Secure Localization Algorithms for Wireless Sensor Networks [Security in Mobile Ad Hoc]," *IEEE Comm. Magazine*, vol. 46, no. 4, pp. 96-101, Apr. 2008.

[14] D. Liu, P. Ning, and W. Du, "Attack-Resistant Location Estimation in Wireless Sensor Networks," *Proc. Fourth Int'l Workshop Information Processing in Sensor Networks (IPSN '05)*, pp. 99-106, Apr. 2005.

[15] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," *Proc. Fourth Int'l Workshop Information Processing in Sensor Networks (IPSN '05)*, pp. 91-98, Apr. 2005.

[16] C. Wang, A. Liu, and P. Ning, "Cluster-Based Minimum Mean Square Estimation for Secure and Resilient Localization in Wireless Sensor Networks," *Proc. Int'l Conf. Wireless Algorithms, Systems and Applications (WASA '07)*, pp. 29-37, Aug. 2007.

[17] D. Liu, P. Ning, and W. Du, "Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks," *Proc. 25th Int'l Conf. Distributed Computing Systems (ICDCS '05)*, pp. 609-619, 2005.

[18] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation-Based Beacon Trust System," *Proc. Second IEEE Int'l Symp. Dependable, Autonomic and Secure Computing (DASC '06)*, pp. 277-283, 2006.

[19] W. Du, L. Fang, and P. Ning, "Lad: Localization Anomaly Detection for Wireless Sensor Networks," *J. Parallel and Distributed Computing*, pp. 874-886, 2006.

[20] N. Sastry, U. Shankar, and D. Wagner, "Secure Verification of Location Claims," *Proc. ACM Workshop Wireless Security (WiSe '03)*, pp. 1-10, Sept. 2003.

[21] L. Lazos and R. Poovendran, "Serloc: Robust Localization for Wireless Sensor Networks," *ACM Trans. Sensor Networks*, vol. 1, no. 1, pp. 73-100, Aug. 2005.

[22] S. Capkun and J. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," *Proc. IEEE INFOCOM '05*, vol. 3, pp. 1917-1928, 2005.

[23] L. Lazos, S. Capkun, and R. Poovendran, "Robust Position Estimation in Wireless Sensor Networks," *Proc. Fourth Int'l Workshop Information Processing in Sensor Networks (IPSN '05)*, pp. 324-331, Apr. 2005.

[24] A. Savvides, C. Han, and M. Srivastava, "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," *Proc. ACM MobiCom '01*, pp. 166-179, July 2001.

[25] D. Xu and K.E. Ygard, "Threat-Driven Modeling and Verification of Secure Software Using Aspect-Oriented Petri Nets," *IEEE Trans. Software Eng.*, vol. 32, no. 4, pp. 265-278, Apr. 2006.

[26] T. Murata, "Petri Nets: Properties, Analysis and Applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541-580, 1989.

Daojing He received the BS degree from the Harbin Institute of Technology in 2007. He is currently working toward the MS degree at the Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China. His research interests include wireless networks, speech signal processing, information retrieval, and so forth.

Lin Cui received the BS degree from Shandong University, Weihai, China, in 2007. He is currently working toward the MS degree at the Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China. His general research interest falls in the area of wireless ad hoc network.

Hejiao Huang received the PhD degree from the City University of Hong Kong in 2004. She is currently an associate professor at the Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China and is an invited professor at INRIA, Bordeaux, France. Her research interests include wireless communication networks, formal methods for software system design, Petri net theory and applications, and so forth. She is a member of the IEEE.

Maode Ma received the BE degree in computer engineering from Tsinghua University in 1982, the ME degree in computer engineering from Tianjin University in 1991, and the PhD degree in computer science from Hong Kong University of Science and Technology in 1999. He is an associate professor in the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He has extensive research interests including wireless networking, optical networking, grid computing, bioinformatics, and so forth. He has been a member of the technical program committee for more than 70 international conferences. He has been a technical track chair, tutorial chair, publication chair, and session chair for more than 40 international conferences. He has published more than 120 international academic research papers on wireless networks and optical networks. He currently serves as an associate editor for *IEEE Communications Letters*, an editor for *IEEE Communications Surveys and Tutorials*, an associate editor for the *International Journal of Wireless Communications and Mobile Computing*, an associate editor for the *International Journal of Security and Communication Networks*, and an associate editor for the *International Journal of Vehicular Technology*. He is a member of the IEEE.