Trust-based Mutual Authentication for Bootstrapping in 6LoWPAN

Hong Yu
College of Computer Science and Technology,
Beijing University of Technology, Beijing 100124, China
Email: yuhong_0826@emails.bjut.edu.cn

Jingsha He
School of Software Engineering,
Beijing University of Technology, Beijing 100124, China
Email: jhe@bjut.edu.cn

***Abstract*—IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) has emerged as a promising technology to realize ambient intelligence under the vision of the Internet of Things. Under most circumstances, it is imperative that security be addressed from bootstrapping to data transmission. In this paper, we propose a secure bootstrapping scheme that includes mutual authentication and trust evaluation to provide the first security measure for 6LoWPAN. The scheme is based on multi-hop cluster-tree hierarchical topology in which pairwise keys between neighboring nodes and trust paths to the base station (BS) are established at the same time. Mutual authentication that is based on pairing requires only the storage of one key and the exchange of IDs considering the computational complexity of public key algorithms and the frangibility of shared key protocols. Trust evaluation relies on multiple criteria to achieve security and energy efficiency and to balance the whole network. The BS also maintains a dynamic blacklist to prevent denial of service (DoS) attacks. Analysis shows that the proposed scheme is secure and scalable. The energy cost in terms of computation and communication as well as storage are also analyzed and compared to that of shared key protocols and public key algorithms through quantitative analysis.**

***Index Terms*—6LoWPAN, security, bootstrapping, mutual authentication, trust evaluation**

I. INTRODUCTION

With the development of wireless sensor network (WSN) technology, the futuristic vision of the Internet of Things has emerged in which all things on the earth can communicate with each other. Therefore, it has become increasingly more important to ensure the accessibility of nodes in a sensor network over IP, especially IPv6, in the near future. However, with the characteristics of small size and limited power, storage and calculation capability, a sensor node is a conundrum for the classic IPv6 protocol stack. To deal with this limitation, a new protocol, i.e., 6LoWPAN, has been proposed by IETF 6LoWPAN Working Group to enable most capabilities of IPv6 in a resource-constrained node [1] and the transmission of IPv6 packets over low power wireless personal area networks based on IEEE 802.15.4 standard [2]. 6LoWPAN has probably paved the way for the implementation of the Internet of Things.

6LoWPAN is designed to support a variety of applications ranging from defense systems to health care, industrial monitoring, disaster management, home automation, and so on [3]. Many of the applications have certain security requirements from bootstrapping to data transmission. Therefore, the 6LoWPAN Working Group has viewed security design as one of the goals and set some security requirements such as secure bootstrapping and key management [4]. However, feasible solutions are still yet to be proposed.

Normally, any node within the range of radio wave may access the 6LoWPAN, resulting in fatal consequence to military applications. In addition, in many industrial and consumer applications, it requires that monitoring data be kept private from adversaries. Therefore, it is necessary to implement authentication of a new node when it tries to join the network at the time of bootstrapping to guard against intruders and to avoid interactions with nodes from a neighboring network.

Bootstrapping includes all steps that make a node become part of a network, which at the least consists of making aware of the presence of a new node to the BS or other existing nodes, getting basic information about the personal area network (PAN), exchanging security credentials and passing authentication phase, establishing pairwise keys with neighboring nodes as well as trust paths to the BS, and getting an IPv6 address finally. However, huge energy consumption during the bootstrapping phase can shorten the total life of the network because in many applications, the replacement of the batteries is not possible after deployment. More specifically, the number of messages that are exchanged, the storage in each node and the amount of computation must be kept as low as possible. In general, secure bootstrapping should meet the following two

Manuscript received August 31, 2011; revised December 22, 2011; accepted April 16, 2012.

doi:10.4304/jcm.7.8.634-642

requirements: (1) at deployment, attackers cannot access the network and acquire sensitive information even by eavesdropping on network's radio frequency; (2) after deployment, the impact of node compromise cannot spread across the entire network and new nodes can join at any time without any impact to existing nodes.

However, energy and resource constraints in sensor nodes present a great challenge for proposing secure bootstrapping schemes in 6LoWPAN. To prevent unauthorized nodes from joining a PAN, authentication of a new node is essential to meet the first requirement. On the other hand, authentication schemes designed for the Internet cannot be applied directly to 6LoWPAN due to the complexity of Public Key Infrastructure (PKI). Meanwhile, shared key mechanisms are too vulnerable to resist node compromise attacks to meet the second requirement. Therefore, lightweight and robust authentication schemes should be considered for bootstrapping in 6LoWPAN.

In this paper, we present a secure bootstrapping scheme that can meet the above requirements while taking into consideration the energy constraint of the sensor nodes. When a sensor node is trying to join the network, it must pass mutual authentication and establish pairwise keys with its authenticated neighboring parents. Multiple criteria will be used in our scheme for the node to choose the most trusted node from authenticated parents to establish a trust path to the BS.

The remainder of this paper is structured as follows. In the next section, we review some related work on bootstrapping schemes for 6LoWPAN as well as on methods for authentication in sensor networks and for trust evaluation. In Section III, we present our bootstrapping scheme in which we describe 6LoWPAN topology and assumptions as well as protocols for authentication and trust evaluation. In Section IV, we analyze the security, salability and energy consumption of the proposed scheme. Finally, we conclude this paper in Section V in which we also discuss some future work.

II. Related Work

Research on bootstrapping in 6LoWPAN is still in the initial stage and Neighbor Discovery (ND) of 6LoWPAN [5] has not been standardized yet. The 6LoWPAN Working Group of IETF is working on some issues for bootstrapping such as reducing the amount of ND multicast traffic and allowing a single subnet to span multiple routers. However, no mechanism has been proposed for authenticating a new node. Moreover, if more than one 6LoWPAN routers relay registration messages to the new node, there is no specification regarding how the new node can select the best router to join the PAN.

A. Bootstrapping schemes for 6LoWPAN

There are currently two bootstrapping schemes designed specifically for 6LoWPAN. Ikram et al. proposed a simple lightweight authentic bootstrapping scheme for 6LoWPAN which is independent of any key management infrastructure [6]. The scheme uses pre-shared keys in conjunction with a shared secret code for mutual authentication. The unique shared authentication key between a parent node A_i^k and an immediate child node A_{i+1}^k in hierarchical authentication tree and the message authentication code (MAC) can be computed as follows:

$$K_i^a = AES^{j+1}(AES^j(SID,R) \oplus Co_i^a) \quad (1)$$

$$MAC_{A_{i+1}^k} = CAES_i^j(K_i^a, R_{A_i^k} \| ID_{A_i^k} \| R_{A_{i+1}^k} \| ID_{A_{i+1}^k}) \quad (2)$$

$$MAC_{A_i^k} = CMACAES_i^j(K_i^a, ID_{A_i^k} \| R_{A_{i+1}^k}) \quad (3)$$

At either side, the parent A_i^k or the immediate child A_{i+1}^k, K_i^a is generated from the system identifier $SID \in \{A_i^k \cup A_{i+1}^k\}$ in conjunction with a shared random challenge $R \in \{R_{A_{i+1}^k} \cup R_{A_i^k}\}$ by using the AES counter mode recursive operations.

The mutual authentication process can be described as follows:

$$A_{i+1}^k \rightarrow A_i^k : \text{“registration”}, ID_{A_{i+1}^k}, N_{A_{i+1}^k} \quad (4)$$

$$A_i^k \rightarrow A_{i+1}^k : \text{“reg. reply”}, \ ID_{A_i^k}, N_{A_i^k}, R_{A_i^k} \quad (5)$$

$$A_{i+1}^k \rightarrow A_i^k : ID_{A_{i+1}^k}, ID_{A_i^k}, N_{A_{i+1}^k}, N_{A_i^k}, R_{A_{i+1}^k}, R_{A_i^k}, MAC_{A_{i+1}^k} \quad (6)$$

In the above scheme, since Step (4) is not authenticated, an attacker can inject fake registration messages to legitimate node A_i^k to launch a resource exhausting attack. Moreover, legitimate node A_i^k would finish at Step (5). So, the malicious node may never execute Step (6), which will cause DoS attacks. In addition, this scheme failed to consider how a child node would select the best parent to join the PAN if more than one parents relay the registration message to the child node.

Cha et al. proposed a secure and efficient network bootstrapping protocol for 6LoWPAN, called LBP, in which three different kinds of nodes are defined: new device (LBD), already bootstrapped device (LBA) and gateway or PAN coordinator (LBS) [7]. In the protocol, LBS is the only node that makes the decision about whether an LBD should be allowed to join the PAN and the LBA helps the LBD to communicate with LBS. To solve the problems that are not considered by the scheme in [6], the LBA selection algorithm is as follows:

$$\text{LBD} \rightarrow \text{LBA: “LBA Solicitation”}, ID_{LBD} \quad (7)$$

$$\text{LBA} \rightarrow \text{LBD: “LBA advertisement”}, ID_{LBA}, \text{node\_type, hop\_dist, child\_num} \quad (8)$$

When an LBA receives a message, it first checks its blacklist table and, if this LBD is not found there, it will broadcast the “LBA advertisement” message which includes ID_{LBA}, its type (LBS or LBA), its hop count

from the LBS and the number of LBDs it has already served. The LBD will select the best LBA if there are more than one LBA. The LBD would select the LBS if there is a direct advertisement from it. Otherwise, it would check the hop count of an LBA to the LBS and choose the LBD with the minimum distance to the LBS. The selected LBA will forward an "LBP request" message to the LBS. However, the authentication between the LBS and the LBP is omitted.

The LBP scheme uses a blacklist to prevent DoS attacks in the bootstrapping process. When LBS receives an "LBP request" message but the LBD doesn't pass the authentication procedure, the LBS would insert a new entry in the blacklist table for the LBD or increase the number of illegal tries for the LBD. If the number of illegal tries exceeds a defined threshold, the LBS will identify the LBD as a DoS attacker. Whenever a new LBD is determined to be an attacker, the LBS broadcast the blacklist table to all LBAs. Because every LBD must be authenticated by the LBS, the communication overhead is high and the LBS can be a single point of failure for network security. Let us consider the case in which an attacker broadcasts an "LBA Solicitation" message with a fresh illegal ID constantly. LBAs must broadcast this kind of unencrypted messages which can be easily exploited by the attacker. Because authentication is performed after LBA selection algorithm, the LBA must broadcast the "LBA advertisement" message constantly. However, the attacker may never execute the next step, which will cause another form of DoS attacks.

We can see from the above analysis that mutual authentication and parent selection are essential. It is also imperative that DoS attacks be blocked at the first step in the phase of new node registration.

B. Authentication in sensor networks

Authentication can be achieved by using two types of messages: MAC and digital signature.

MAC is based on pre-distributing shared keys or performing shared key agreement. The sender uses the shared key to generate a MAC that can be verified by the receiver. Computation overhead for symmetric key cryptography is very low.

Digital signature allows a sender to generate a signature with its private key on a message. The receiver can verify the authenticity of the signature with the sender's public key to ensure that the massage indeed originates from the claimed sender and has not been modified. Verification causes more computational complexity than signing. Moreover, it would consume more time and energy to sign and verify a message than to compute a MAC.

Based on the characteristics of communication devices and the current 6LoWPAN, such as limited resources and lack of physical protection, some authentication protocols have been proposed based mainly on public key algorithms using digital signature and shared key protocols using MAC.

Watro et al. presented an authentication protocol based on RSA called Tiny PK which needs PKI [8] in which the BS is treated as a Certificate Authority (CA). Sensor nodes perform encryption and verification by using public keys while decryption and signature are implemented by the BS by using private keys or other exterior devices that have sufficient energy. This scheme cannot be applied to authenticating a sensor node because RSA consumes a lot of energy, so do decryption and signature by using private keys. Moreover, if one node is compromised, the whole network will be in danger and attackers can join the network as legitimate nodes though the compromised node.

Benenson et al. proposed RRUA [9], an authentication protocol based on ECC, in which a node must broadcast an authentication request to n nodes among which t nodes will certify and respond (n is the average number of nodes within the communication range of an authenticating node and t is the threshold for the number of captured nodes). Although ECC consumes less energy than RSA does, the protocol cannot defend DoS attacks effectively since a node must complete five steps to detect an attacker that keeps sending forged certification to it.

Oliveira et al. presented the TinyPBC scheme that uses pairings for the distribution of authenticated identity-based keys in sensor networks [10]. By only knowing the ID of the other, two parties can agree on keys without any interaction.

The first two authentication schemes are based on public key certificates while the last one is based on identity, making certificates unnecessary. However, a trusted third party knows the secret keys of all the nodes. In the case of 6LoWPAN, the trusted third party is the deployer of the network. Consequently, there is little doubt in its trustworthiness.

Authentication protocols based on shared key algorithms in sensor networks have taken two extreme forms. One simple idea is that all the nodes in the network share one key for communication. In this case, if one node is compromised, the entire network is in danger. The other extreme is that each node (assuming that there are n nodes) stores n-1 keys each of which is shared with each of the other n-1 nodes. Therefore, it requires a large amount of storage in each node in a large scale network and may result in waste because not every node can communicate with every other node. In addition, if a new node enters the network after deployment, new keys must be issued that involve all the nodes.

Zhu et al. proposed LEAP protocol [11] using only symmetric primitives for single hop communication which is perhaps the most efficient proposal. In the protocol, a new node u authenticates its neighboring node v using v's individual key K_v derived through $K_v=f(K, ID_v)$ where K is a pre-shared master key. However, LEAP has some drawbacks. Firstly, LEAP assumes that a pre-distributed key is shared among all the nodes and won't be disclosed during the t initial time units of network operation. Secondly, LEAP assumes that once this pre-distributed key is erased, it cannot be recovered from memory. However, this cannot always be guaranteed. Lastly, LEAP does not provide digital

authentication and repudiation of messages is still possible.

Bauer et al. proposed a distributed authentication protocol that makes use of secret sharing and the cryptographic concept of group agreement [12]. A new node and the BS share a key S which is divided into n-1 parts by the BS and distributed to n-1 nodes except the new node. All the nodes send their partial keys to a specified node who reverts the original key S' and compares it with S from the new node. The specified node then broadcasts a relay message. If any node receives n-2 copies of the relay message and among which more than half are determinate, the new node is authenticated. Since there is no encryption or decryption involved, it has a good performance on fault tolerance and computation. However, it requires that all nodes within a group communicate collaboratively, which may cause data collision when all the nodes are sending determinate messages.

C. Trust evaluation

The 6LoWPAN ND draft goes to standardize the registration messages but doesn't address how a new node can find the edge router. Moreover, if there are more than one 6LoWPAN routers that can relay the registration message to the edge router, a decision has to be made as to which 6LoWPAN router or routers will relay the message or how a new node can select the best 6LoWPAN router.

In the bootstrapping phase, after deployment, beginning with the BS, sensor nodes gradually join the network and a cluster-tree structure could be formed. After a node sends out a registration message, it may receive one or more response messages from nodes located in the higher hierarchy. It is necessary for the node to authenticate reciprocally and choose the most trusted one to access the network. Simply considering energy [13] or hop counts from the BS [14] may not achieve desired security and efficiency. We propose to compute the trust value of every legal parent based on four factors: hop count from the BS, number of children, consumed energy and delay. Making use of the utility value method in a multiple criteria decision making scheme from the perspective of simplicity and energy efficiency can make the network more secure and effective from the beginning.

III. The Proposed Scheme

A. 6LoWPAN topology

A 6LoWPAN network consists of one or more PANs of full function devices (FFDs) and reduced function devices (RFDs). The 6LoWPAN standard supports star and peer-to-peer topologies. In a star topology, FFDs and RFDs communicate with a single central PAN coordinator whose role can be represented by a FFD. FFDs are responsible for communication within the network while RFDs can only serve as end nodes. In a peer-to-peer topology, FFDs and RFDs can communicate with each other directly. There are therefore two types of topology: mesh and cluster-tree.

In this paper, a multi-hop cluster-tree hierarchical network topology is assumed. The BS that acts as a PAN coordinator is the root of the whole tree while all the FFDs and RFDs are the children nodes that can form many sub-trees in which only FFDs can be the roots. Fig. 1 shows a cluster-tree consisting of BS, FFDs and RFDs.

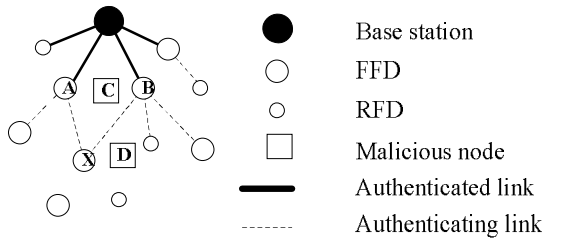

Figure 1. A multi-hop cluster-tree hierarchical network topology

B. Assumptions

We assume that intruders may exist in the target area before deployment or at the bootstrapping phase. These intruders can passively eavesdrop on network's radio frequency and collect transmission data. Moreover, they can also tamper or forge messages. We also assume that nodes that have already been authenticated by higher level parents are trusted at the bootstrapping phase.

C. The proposed scheme

By considering the computational complexity of public key algorithms and the frangibility of shared key protocols, we decide to combine the two authentication approaches in our proposed scheme. At the deployment phase, a unique secret key based on ID is generated for each node. This requirement may be considered high in computational cost, but it has no impact to the network because key generation is performed before deployment. Furthermore, we only use the key as a secure bootstrapping mechanism. Once the nodes are bootstrapped securely, they can use the authenticated shared pairwise key as a static and long-term key to derive the session keys within their own neighborhood.

The proposed secure bootstrapping protocol is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) that builds on Identity-Based Cryptography (IBC) and pairings. The protocol consists of two phases. The first phase takes place before deployment. During this phase, each node is preloaded with the information to be used for authentication and key generation. After deployment, identity and pairings-based mutual authentication is performed to establish the pairwise key between neighboring nodes. For the child node, then, trust evaluation is performed to select the most trusted parent to establish a path to the BS while other paths are kept in trust tables as the optional paths for the future.

Before the deployment of the sensor nodes, the deployer performs the following tasks:

- Choose an additive group G_1 and a multiplicative group G_2 of the same prime order q. Let P be an arbitrary generator of G_1. Then, a bilinear map $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ and two collision resistant cryptographic hash

functions H_1 and H_2 are determined where $H_1:\{0,1\}^* \rightarrow G_1$, a mapping from arbitrary-length strings to points in G_1; $H_2:\{0,1\}^* \rightarrow \{0,1\}^m$, a mapping from arbitrary-length strings to m-bits fixed length output.

- Pick a random number $s \in Z_q^*$ as the master key to identify the network. No one in the network knows this key except the deployer.
- Use the master key s to generate a secret key S for every node in the network. The public and the secret keys for node i is $P_i=H_1(ID_i)$ and $S_i=[s]P_i=[s]H_1(ID_i)$, respectively.
- Preload each node in the network with a unique ID and the corresponding secret key S.

All the nodes are powered on and deployed into the target area. Starting from the BS, all the nodes then gradually join the network.

Only a legitimate child can compute the shared pairwise key with its parent and generate an authentication message to correctly respond to the challenge from the parent and hence authenticate itself and vice versa.

- Node X broadcasts the registration message "Reg"=(ID_X, N_X) that contains the unique ID of X and a nonce. Here, || represents the string concatenation. To prevent two or more nodes from attempting to transmit at the same time, every node would implement a binary exponential backoff algorithm to avoid collisions before broadcasting its "Reg" message.

$$X \rightarrow *: \text{“Reg”}, ID_X, N_X, H_2(ID_X||N_X) \quad (9)$$

- Within the transmission range of "Reg", one or more FFDs who have joined the network may receive it, say nodes A and B, while illegitimate nodes C (to impersonate on a legitimate parent node) and D (to impersonate on a legitimate node X) may also exist, as shown in Figure 1. First, A and B will check their own blacklists and, if there is already a record for X, will discard the "Reg" message. Otherwise, they will validate N_X to fight against replay attacks to ensure the freshness of data and then check $H_2(ID_X||N_X)$ to ensure the integrity of the message. They then respond to node X. Take node A as an example. A will generate a random number R_A and send "Res"=(ID_A, R_A, ID_X, N_X) to X.

$$\begin{aligned} &A \rightarrow X: \text{“Res”}, ID_A, R_A, ID_X, N_X, \\ &\quad H_2(ID_A||R_A||ID_X||N_X) \\ &B \rightarrow X: \text{“Res”}, ID_B, R_B, ID_X, N_X, \\ &\quad H_2(ID_B||R_B||ID_X||N_X) \end{aligned} \quad (10)$$

- After X receives the "Res" messages, it checks N_X to ensure that the "Res" is a response to its registration. X then computes shared keys $K_{X,i}$ with A and B, respectively, according to (11) and generates authentication messages AM_{Xi}, respectively, where $AM_{XA}=MAC(K_{X,A}, ID_A||ID_X||R_A)$ and $AM_{XB}=MAC(K_{X,B}, ID_B||ID_X||R_B)$. Then, X generates the random challenge numbers R_{XA} and R_{XB}, respectively, and sends the authentication messages "Am" to A and B.

$$\begin{aligned} K_{X,A}&=\hat{e}(S_X, P_A)=\hat{e}(Sx, H_1(ID_A)) \\ K_{X,B}&=\hat{e}(S_X, P_B)=\hat{e}(Sx, H_1(ID_B)) \end{aligned} \quad (11)$$

$$\begin{aligned} &X \rightarrow A: \text{“Am”}, ID_X, N_X, ID_A, R_A, R_{XA}, \\ &\quad AM_{XA}, H_2(ID_X||N_X||ID_A||R_A||R_{XA}||AM_{XA}) \\ &X \rightarrow B: \text{“Am”}, ID_X, N_X, ID_B, R_B, R_{XB}, \\ &\quad AM_{XB}, H_2(ID_X||N_X||ID_B||R_B||\ R_{XB}||AM_{XB}) \end{aligned} \quad (12)$$

- A computes the shared key $K_{A,X}$ with X according to (13) as well as a check message $CM_{AX}=MAC(K_{A,X}, ID_A||ID_X||R_A)$. A checks the authenticity of X by matching the received AM_{XA} with its own computed CM_{AX}. If they match, A takes X as a legitimate node and then computes an authentication message AM_{AX}: $AM_{AX}=MAC(K_{A,X}, ID_A||ID_X||R_A||R_{XA})$ with the random number generated by X while responding to A. Otherwise, A silently discards the messages sent by X and terminates the authentication process. In addition, A will report to the BS that X is an illegitimate node.

$$\begin{aligned} K_{A,X}&=\hat{e}(S_A, P_X)=\hat{e}(S_A, H_1(ID_X)) \\ K_{B,X}&=\hat{e}(S_B, P_X)=\hat{e}(S_B, H_1(ID_X)) \end{aligned} \quad (13)$$

$$\begin{aligned} &A \rightarrow X: \text{“Cm”}, ID_A, ID_X, N_X, AM_{AX}, \\ &\quad H_2(ID_A||ID_X||N_X||AM_{AX}) \\ &B \rightarrow X: \text{“Cm”}, ID_B, ID_X, N_X, AM_{BX}, \\ &\quad H_2(ID_B||ID_X||N_X||AM_{BX}) \end{aligned} \quad (14)$$

- X computes a check message CM_{XA}: $CM_{XA}=MAC(K_{X,A},ID_A||ID_X||R_A||R_{XA})$ and compares it with AM_{AX}. If they match, X adds A to its trust evaluation group and requests A to send data. Let's denote the time as TS_A.

A potential parent who receives the request message will generate a reply message. A prepares "Rep"=(ID_A, HN_A, CN_A, CE_A, R_A) that contains ID, hop count from the BS, number of children, consumed energy and the original random number sent to X. So does node B. While HN and CN are obvious, how CE is computed deserves some mentioning.

In 6LoWPAN, energy consumption is determined by communication and computation. The communication cost for a node is related to transmission voltage (Tv), transmission electricity (Te) and transmission speed (Ts). The computational cost for a node is mainly on computing the shared key using a pairing operation which may be different due to the style of nodes. We assume that computing a pairing operation consumes p_c and the number of pairing operations is p_n. Then, the

computational cost is p_c*p_n. So, a rough estimation of consumed energy for a node is "CE"

$$CE=Tv*Te*k/Ts + p_c* p_n \quad (15)$$

where k is the total number of transmission bits.

If CE exceeds CE_{max} or HN exceeds HN_{max}, where CE_{max} and HN_{max} are defined by the network deployer, the FFD won't send a reply message to X.

$$A\rightarrow X: \text{"Rep"}, E_{K_{A,X}}(ID_A,HN_A,CN_A,CE_A,R_A), H_2(E_{K_{A,X}}(ID_A,HN_A,CN_A,CE_A,R_A))$$

$$B\rightarrow X: \text{"Rep"}, E_{K_{B,X}}(ID_B,HN_B,CN_B,CE_B,R_B), H_2(E_{K_{B,X}}(ID_B,HN_B,CN_B,CE_B,R_B)) \quad (16)$$

Trust evaluation by X on its parents is performed following the following steps:

- X records time TR_X as soon as it receives a "Rep" message and deals immediately with it if TR_X doesn't exceed TS_X+TD_{max}, where TD_{max} is defined by the network deployer and is the maximum time delay that can be tolerated by any node. Otherwise, X discards the message. If X doesn't receive any "Rep" message within time interval TD_{max}, it will request A and B to resend the messages. X then computes the trust evaluation value for A and B, respectively, making use of the utility value method in multiple criteria decision making technology.
- X computes the utility value for four criteria. Let's denote $\overline{HN}$ and $\underline{HN}$ as the max and min values of all the HN_i, $\overline{CN}$ and $\underline{CN}$ as the max and min values of all the CN_i, $\overline{CE}$ and $\underline{CE}$ as the max and min values of all the CE_i , and $\overline{TD}$ and $\underline{TD}$ as the max and min values of all the TD_i, and $TD_i=TR_i-TS_i$.

$$U_{HNi} = \frac{\overline{HN}-HN_i}{\overline{HN}-\underline{HN}}, \quad U_{CNi} = \frac{\overline{CN}-CN_i}{\overline{CN}-\underline{CN}}$$

$$U_{CEi} = \frac{\overline{CE}-CE_i}{\overline{CE}-\underline{CE}}, \quad U_{TDi} = \frac{\overline{TD}-TD_i}{\overline{TD}-\underline{TD}} \quad (17)$$

- X computes trust evaluation value. If the weights of HN, CN, CE, TD are a, b, c and d, respectively, that are defined by the network deployer based on application requirements, then

$$Ti=a* U_{HNi} + b* U_{CNi} + c* U_{CEi} + d* U_{TDi} \quad (18)$$

- X chooses the most trusted node which has the largest value of T_i, among all the nodes evaluated and all the others are reserved in the trust table as optional paths for the future.

IV. Protocol Analysis

We now show that our proposed scheme can effectively defend the various major attacks. We also analyze the salability. The energy cost in terms of computation and communication as well as storage are also analyzed and compared to that of shared key protocols and public key algorithms through quantitative analysis.

A. Security analysis

- **Masquerading attacks:** An attacker can pretend to be a valid node to deceive a child node to connect to it or to cheat a parent node to accept its access requests. In our proposed scheme, since nodes authenticate each other along all the links, the attacker cannot become a child because it cannot pass the authentication after (12). Neither can it become a parent due to failure in authentication after (14).
- **Relay attacks:** An attacker can replay the old registration messages to threaten message freshness. In our proposed scheme, this kind of attacks can be prevented because every registration message has a nonce, as shown in (9), that can guarantee the freshness of the message.
- **Eavesdropping, tampering and forging attacks:** An attacker can eavesdrop on the information in the transmission process and then tamper or forge it to threaten message integrity. In our proposed scheme, the hash function H_2 is used to prevent false messages and the information for computing the trust value is encrypted to ensure confidentiality.
- **Capture attacks:** Should an attacker capture a node, it could totally control the node and get the secret key. In our proposed scheme, although we cannot solve the node compromise problem, the attacker cannot get the master key of the whole network due to ECDLP even if the attacker has the secret keys. Therefore, the impact is strictly regional. That is, even if an attacker could compromise a node, it would not get any information about uncompromised nodes.
- **Resource exhaustion and DoS attacks:** Every new node needs to broadcast a "Reg" message periodically to ask for joining the network. If an attacker injects fake "Reg" messages with illegal IDs, FFDs within the coverage of "Reg" need to compute share keys using the illegal IDs, resulting in resource exhaustion and DoS attacks. In our proposed scheme, the BS maintains a blacklist and updates it to all FFDs and thus FFDs can block the attacker.

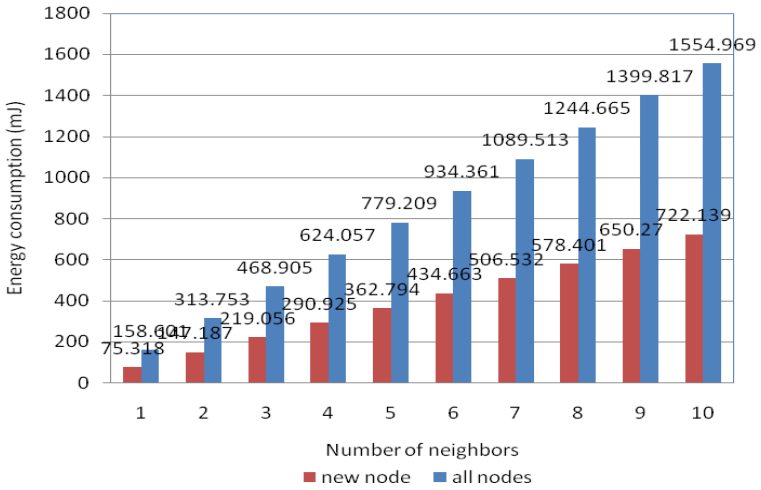

Figure 2. Energy consumption of all the nodes for one authentication

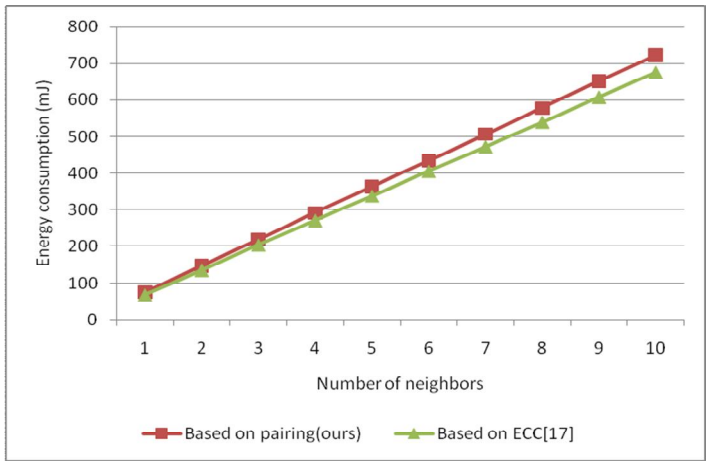

Figure 3. Energy consumption of the new node in our scheme and public key schemes based on ECC

B. *Scalability analysis*

After deployment, it is simple to add more nodes into the network. The new nodes could easily build new trust relationships with existing nodes as the mutual authentication is based only on exchanging IDs. In addition, our scheme supports mobility of the nodes. When a node is disconnected from the original parent, it can act like a new node and perform authentication with a new parent. However, its immediate children will have to register with new parents.

C. *Performance analysis*

In our proposed scheme, energy consumption is determined by communication and computation. Energy consumption is estimated in the process of trust evaluation, as shown in (15). We now perform a quantitative analysis on energy consumption for two FFDs in one mutual authentication process in which we assume that the FFDs have the same capabilities as those of a standard MICA2 mote [15]. MICA2 has the 8-bit ATmegal 128L clocked at about 8-MHz microcontroller and complies with the IEEE 802.15.4 standards. It works on 3V and 8mA. The sending electricity is 27mA while the receiving electricity is 10mA and the data transmission rate is 12.4kbps. According to [16], computing a η_T pairing operation on MICA2 takes 2.66s and consumes 62.73mJ. We also assume that the lengths of the ID, the random number and the nonce are each 2 bytes. Using AES-CBC-MAC-128 mode in the IEEE 802.15.4 standards, the head is then 25+21=46 bytes, the lengths of $H_2()$ and MAC() are each 16 bytes, and the hop count, number of children, consume energy and delay are each 2 bytes. Table I lists the communication cost for each message transmission in terms of both sending and receiving.

TABLE I

THE COST OF COMMUNICATION.

Communication (#)	Length (bytes)	Sending (mJ)	Receiving (mJ)
(9)	66	3.449	1.277
(10)	70	3.658	1.355
(12)	88	4.598	1.703
(14)	84	4.390	1.626
(16)	78	4.076	1.510

Assuming that the number of neighboring nodes that will respond to the "Reg" message broadcast by a new node is N, in Fig. 2, we show the energy consumption of all the nodes including the new node and N parent nodes.

During one mutual authentication process, the energy consumption of the new node and all the other nodes are 3.449+71.869N mJ and 3.449+155.152N mJ, respectively. We can see that the energy consumption is mainly due to the pairing operation. However, with 2 AA batteries of 600mAs in the MICA2 node, the available energy is 2*1.5*800*3600=8640J. Performing one mutual authentication with one neighboring node only consumes 0.009% of the total energy.

Due to the pairing operation, our scheme consumes more energy for authentication than that for the shared key schemes which are much more vulnerable to attacks. However, our scheme requires only the storage of one key and the exchange of IDs, which is the advantage in terms of storage and communication cost.

Fig. 3 shows the comparison between the public key schemes based on ECC [17] and our proposed scheme for authentication. We can see from Fig. 3 that energy consumption of the new node in our scheme based on pairing is slightly more than that for the public key schemes based on ECC which requires two point multiplication for node authentication and one point multiplication for computing the pairwise key. According to [18], completing a 160-bit point multiplication of ECC is 0.81s in the MICA2 mote. Therefore, the computing cost for the scheme in [17] is 3*8*0.81*3=58.32mJ, which is less than that for the pairing operation. However, our proposed scheme has the advantage of requiring less storage space because the scheme in [17] requires that each node store the private and the public keys, the CA's signature and the CA's public key, with a total reaching more than 100 bytes. In our scheme, the node only needs the storage of its secret key and ID which only requires 24 bytes, thus much less than the storage space required in the scheme in [17].

V. CONCLUSION

In this paper, we proposed a secure bootstrapping scheme for 6LoWPAN that is comprised of pairing based mutual authentication and trust evaluation. Analysis on the proposed scheme showed that the scheme can effectively defend against various major attacks. In addition, our bootstrapping protocol relies on a hierarchical cluster-tree structure based on 6LoWPAN and, therefore, can scale well into a large network and is adaptable to a relatively less mobility scenario. Quantitative analysis of energy consumption showed that although our scheme based on pairing is a little more complex than protocols that are based on ECC in computation and communication, the storage requirement for each node is much less than that based on ECC. In the future, we will further optimize the trust evaluation model and verify our scheme in real applications. We will also study security issues to confront after the completion of bootstrapping, such as key management, intrusion detection, etc.

REFERENCES

[1] N. Kushalnagar, G. Montenegro and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," IETF RFC 4919, Aug. 2007.

[2] G. Montenegro, N. Kushalnagar and J. Hui, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF RFC 4944, Sept. 2007.

[3] R. Riaz, K. Ki-Hyung and H. F. Ahmed, "Security Analysis Survey and Framework Design for IP Connected 6LoWPANs," Proc. International Symposium on Autonomous Decentralized Systems, Athens, Greece, Mar. 2009, pp.1-6.

[4] S. D. Park et al., "IPv6 over Low Power WPAN Security Analysis draft-6lowpan-security-analysis-05," IETF Internet Draft, Mar. 2011.

[5] Z. Shelby et al., "Neighbor Discovery Optimization for Low Power and Lossy Networks (6LoWPAN) draft-ietf-6lowpan-nd-17," IETF Internet Draft, Jun. 2011.

[6] M. Ikram et al., "A Simple Lightweight Authentic Bootstrapping Protocol for IPv6-based Low Rate Wireless Personal Area Networks (6LoWPANs)," Proc. ACM International Wireless Communications and Mobile Computing Conference, Leipzig, Germany, Jun. 2009, pp. 937-941.

[7] H. Cha, K. Kim and S. Yoo, "LBP: A Secure and Efficient Network Bootstrapping Protocol for 6LoWPAN," Proc. 5th International Conference on Ubiquitous Information Management and Communication, Seoul, Korea, Feb. 2011.

[8] R. Watro et al, "TinyPK: Securing Sensor Networks with Public Key Technology," Proc. 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington, DC, Oct. 2004, pp. 59-64.

[9] Z. Benenson, N. Gedicke and O. Raivio, "Realizing Robust User Authentication in Sensor Networks," Proc. Workshop on Real-World Wireless Sensor Networks, Stockholm, Sweden, Jun. 2005.

[10] L. B. Oliveira, M. Scott, J. Lopez and R. Dahab. "TinyPBC: Pairings for Authenticated Identity-based Non-interactive Key Distribution in Sensor Networks," Computer Communications, vol. 34, no. 3, Mar. 2011, pp. 485-493.
[11] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks," Proc.10th ACM Conference on Computer and Communications Security, Washington, DC, Oct. 2003, pp. 62-72.
[12] K. Bauer and H. Lee, "A Distributed Authentication Scheme for a Wireless Sensing System," ACM Transactions on Information and System Security, vol. 11, no. 3, Mar. 2008, pp. 1-35.
[13] H. Song, S. H. Lee and H. S. Lee, "6LoWPAN-based Tactical Wireless Sensor Network Architecture for Remote Large-scale Random Deployment Scenarios," Proc. IEEE Military Communications Conference, Boston, MA, Oct. 2009, pp.1-7.
[14] K. Zeng, K. Ren, W. Lou and P. J. Moran, "Energy Aware Efficient Geographic Routing in Lossy Wireless Sensor Networks with Environmental Energy Supply," Wireless Networks, vol. 15, no. 1, Jan. 2009, pp. 39-51.
[15] Crossbow, "MICA2", http://www.xbow.com/Products /Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf.
[16] P. P. Szczechowiak, A. Kargl, M. Scott and M. Collier, "On the Application of Pairing based Cryptography to Wireless Sensor Networks," Proc. 2nd ACM Conference on Wireless Network Security, Zurich, Switzerland, Mar. 2009, pp. 1-12.
[17] X. Zhang, J. He and Q. Wei, "EDDK: Energy-Efficient Distributed Deterministic Key Management for Wireless Sensor Networks," EURASIP Journal on Wireless Communications and Networking, vol. 2011, Jan. 2011.
[18] N. Gura, A. Patel, A. Wander, H. Eberle and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs," Proc. 6th International Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, MA, Aug. 2004, pp. 119-132.

Hong Yu was born on 21th September 1984 in Hunan province, China. She received her Master's degree in Computer Science and Technology in 2011 from Beijing University of Technology in Beijing, China and is currently a Ph.D. student there. Her research interest is mainly in the area of security and privacy in wireless sensor networks.

Jingsha He was born on 15 April 1961 in China. He received his M.S. and Ph.D. degrees from the University of Maryland, USA in 1984 and 1990, respectively. He joined Beijing University of Technology in Beijing, China in 2003 and is currently a professor in the university. Prof. He's research interests are mainly in the areas of security and privacy in wireless networks, network measurement and information security. He has received 12 U.S. patents and 11 China patents and has published extensively in technical journals and major international conferences.