Authentication and En-route Data Filtering for Wireless Sensor Networks in the Internet of Things Scenario

Hong Yu[1] and Jingsha He[2*]

[1]*College of Computer Science and Technology*
Beijing University of Technology, Beijing 100124, China
[2]*School of Software Engineering*
Beijing University of Technology, Beijing 100124, China

yuhong_0826@emails.bjut.edu.cn, jhe@bjut.edu.cn

Abstract

To become an indispensable part of the Internet of Things (IoT), wireless sensor networks (WSNs) have to be integrated into the Internet. Under such circumstances, any IP-enabled node in the Internet shall be able to directly communicate with any sensor node in a WSN. Then, multiple sensor nodes can be used to monitor an event and jointly generate a report to be sent to one or more Internet nodes for monitoring purposes. Hence, it becomes imperative that every event report that is transmitted from within the WSN be authenticated to intended Internet users and efficiently filtered on its way to the Internet users. However, most present authentication and en-route data filtering schemes developed for WSNs don't consider the Internet scenario while traditional mechanisms developed for the Internet can hardly be suitable due to resource constraints of sensor nodes in WSNs. In this paper, we propose an authentication and en-route data filtering scheme for WSNs in the IoT scenario in which signature shares based on the most efficient ID-based signature scheme are generated and distributed by making use of verifiable secret sharing cryptography. Security analysis shows that the proposed scheme can defend against node compromise attacks as well as denial of service (DoS) attacks that cause report disruption and selective forwarding problems. Energy consumption as the result of computation and communication is also analyzed to show the advantages of our scheme compared to some other comparable schemes.

Keywords: *Internet of Things (IoT), wireless sensor network (WSN), authentication, en-route filtering, denial of service (DoS) attacks*

1. Introduction

To become an indispensable part of the Internet of Things (IoT), wireless sensor networks (WSNs) need to adopt IP technologies to create a seamless, global network infrastructure together with the Internet. To achieve this goal, many standardization organizations have been actively pursuing standardization work. IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) is one such technology that the Internet Engineering Task Force (IETF) 6LoWPAN Working Group is developing for completely integrating WSNs into the Internet as well as for enabling most of the IPv6 capabilities on resource-constrained nodes [1] and for transmitting IPv6 packets over low power wireless personal area networks based on IEEE 802.15.4 standards [2].

* The Corresponding Author

In the IoT scenario, any IP-enabled node in the Internet shall be able to communicate directly with any remote sensor node in a WSN that is used to monitor specific events. Data transmission from any WSN node to any Internet node can be event-driven, whose scenarios include events that may be sensed sporadically by multiple cooperative sensor nodes when something happens, *e.g.*, when detecting fire or door-opening, or can be scheduled at predefined intervals, *e.g.*, reporting temperature every two hours. The use of more than one sensor to monitor specific events is an effective strategy to improve robustness, especially in an environment in which security threats resulting from external attacks as well as internal attacks due to node compromises become a serious issue. Under such circumstances, it is still required that event data be sent to one or more intended Internet users as accurately as possible.

Since sensor nodes in a WSN may be deployed in an unattended environment, as shown in Figure 1, attackers can relatively easily compromise one or more sensor nodes so that they can be used to inject false event data (*e.g.*, compromised node A can report false data for the event) or disrupt the transmission of legitimate event data (*e.g.*, compromised node B can temper or even discard true data for the event within the multi-hop forwarding process). If undetected, such attacks can cause not only the generation of false alarms but also the depletion of limited energy in the legitimate sensor nodes. Moreover, Internet users may not be notified of a real event quickly and handle the event in time to avoid serious consequences. Therefore, it has become imperative that efficient authentication and en-route data filtering from WSN nodes to one or more Internet users be supported to detect such attacks.

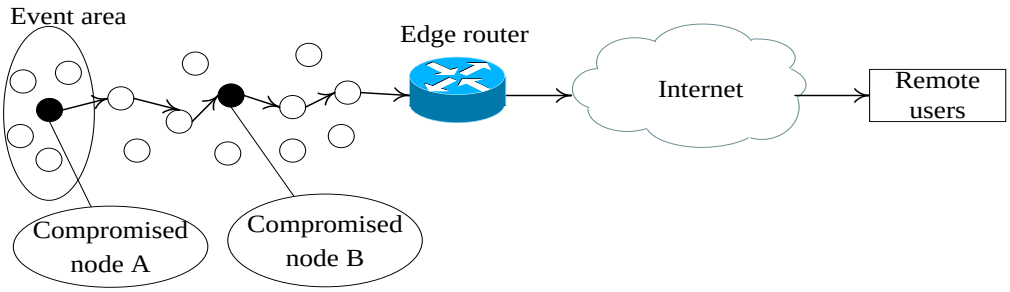

Figure 1. Compromised Nodes Can Inject False Event Data or Disrupt the Transmission of Legitimate Event Data

Traditional detection mechanisms developed for the Internet usually rely on infrastructure equipment (*e.g.*, firewalls) to filter out distributed denial of service (DDoS) packets, which is deemed to be not adequate for WSNs due to the resource-constrained characteristics of sensor nodes as well as the lack of a comparable infrastructure in WSNs. Meanwhile, current detection mechanisms developed for WSNs rely primarily on the use of pre-distributed keys shared between the sensor node and the sink node, which cannot be directly applied to the IoT scenario since the data of the event sensed by cooperative sensor nodes is sent only to one local sink rather than to one or more Internet users who are usually situated in different locations, even in different networks from the cooperative sensor nodes, and who may not be able to establish shared keys with every sensor node to authenticate the event data from a sensor node.

In this paper, we propose an authentication and en-route data filtering scheme for WSNs in the IoT scenario. In the scheme, we make use of verifiable secret sharing cryptography to distribute the shares based on the most efficient ID-based signature scheme to multiple cooperative sensor nodes. In the case of a node compromise, with the tolerance of an

adversary's compromising multiple neighboring nodes in the event area, the event report should be collectively generated, digitally signed and forwarded to one or more intended Internet nodes through multi-path routing.

The rest of this paper is organized as follows. In the next section, we review some related work on authentication and en-route filtering based on symmetric and asymmetric cryptography. In Section 3, we present our proposed scheme, which includes assumptions, threat model and design goals, two preliminaries and finally the procedure of the scheme. In Section 4, we analyze our proposed scheme in terms of security and performance and compare it to the LBCT scheme. Finally, in Section 5, we conclude this paper in which we also discuss some future work.

2. Related Work

2.1. Authentication Frameworks for IoT

There are currently some authentication frameworks for data reports designed specifically for WSNs in the IoT scenario. Oliveira et al. proposed a Secure-TWS scheme to authenticate the communication from a single node to multiple users by using certificate-based signature in which the certification authority (CA) is part of the existing infrastructure in the Internet and, hence, is easy to provide since the Internet users only trust the CA and don't have to allow the CA to impersonate as themselves [4]. When the users receive a data report signed by a sensor node, they download the sensor node's public key and the corresponding certificate from the CA to authenticate the report using signature verification. Yasmin et al. proposed a framework for authenticated broadcast/multicast by the sensor node using the Identity-based Online/Offline Signature (IBOOS) scheme [5]. The offline phase performs most of the signature computations to calculate the partial signature which is stored on sensor nodes. Whenever a sensor node reports an event, it performs minor computations to obtain the final signature based on the partial signature stored on it.

The above two schemes can enable all sensor nodes in the WSNs to send messages to report critical situations and allow every node on the path from the sender node to the receiver users to verify and filter out false data as early as possible without using any shared keys. The computation overhead of the first scheme is lower than that of the second, but it requires higher communication overhead due to the transmission of certificates.

However, these two schemes don't take into consideration of the existence of compromised nodes that may inject false event data as well as can disrupt the transmission of legitimate event data. Firstly, an event may be reported by a single sensor node which may have been compromised but not yet detected, the false report can get propagated to the users who may then mistakenly take incorrect measures. Secondly, should there be a compromised node in the routes to the Internet users, the users might be misled or might even not be able to receive any messages. Therefore, it is necessary to use multiple surrounding sensor nodes to collectively generate a legitimate data report which should also be forwarded to the Internet users via multipath routing.

2.2. Authentication based on Symmetric Cryptography in WSNs

In WSNs, the problem of authenticating an event report collected by multiple sensors to the local sink node has attracted many attentions in recent years. Most of such schemes, such as SEF [6], IHA [7], DSF [8], LBRS [9] and LEDS [10], achieve the purpose by using message authentication codes (MAC) based on symmetric keys.

SEF allows both the sink node and the en-route nodes to authenticate a report that has multiple MACs generated by a cluster attached to it with a certain probability by using the

keys from different partitions in a global key pool. IHA verifies a report that has t+1 pairwise MACs and one compressed MAC attached that are computed by the cluster lead node in a deterministic and hop-by-hop fashion through using pairwise keys between two upper or lower associated nodes that are t+1 hops away. DSF makes the report carry two types of MACs including t R-type MACs generated by the keys from different partitions in a global key pool and t A-type MACs generated by the pairwise keys shared between the associated nodes, and thus the en-route nodes can authenticate the MACs in a greater probability than SEF. LBRS and LEDS utilize location-based keys to authenticate a data report to prevent compromised nodes from breaking the whole WSN even though a certain area of the WSN may have been affected. Both of these schemes assume that all sensor nodes can determine their locations in a short period of time. However, SEF, HIA and LBRS are highly vulnerable to many types of denial of service (DoS) attacks, such as report disruption attacks and selective forwarding attacks, resulting from node compromises in the event area and from the use of a single route from the sensor node to the sink node.

A report disruption attack happens when some nodes intentionally submit corrupted partial MACs, hence disrupting the process of cooperation by causing the real report to be filtered out by some nodes on the forwarding route. A selective forwarding attack can be launched by one or more compromised forwarding sensor nodes to drop a legitimate report.

LEDS tries to deal with these attacks by allowing a whole cell of nodes to forward T shares of a report which can be recovered by the sink node from any t out of T legitimate shares, which makes LEDS resilient to interference from up to T-t compromised nodes in the event area. However, this scheme is not always feasible since it requires that every sensor node be equipped with GPS capability to measure its location even though localization can provide rough estimation on the location for each non-GPS sensor node. It may also incur extra communication overhead and latency.

2.3. Authentication based on Asymmetric Cryptography in WSNs

Some asymmetric cryptographic schemes, such as PDF [11] and LBCT [3], that rely on signature approaches can enable any report, not just the report that is sent to the sink node, to be authenticated and en-route filtered. Moreover, they do not require any pre-shared keys.

PDF leverages Shamir's threshold cryptography and Elliptic Curve Cryptography (ECC) to reject false data packets while LBCT makes use of Identity-based Cryptography (IBC) based on bilinear pairing to bind the private key of each sensor node to both its identity and geographic location. However, PDF is still vulnerable to both report disruption attacks and selective forwarding attacks while LBCT can provide some level of tolerance to both types of attacks. Unfortunately, the bilinear pairing is too expensive for low energy sensor nodes and localization incurs additional communication overhead. In addition, in LBCT, a data report must be co-signed by t nodes out of T nodes in the event area, thus, adversaries have to compromise at least t nodes to inject false data and more than T-t compromised nodes to launch report disruption attacks.

It is worth mentioning that the relationship between t and T involving the report disruption attacks is not fully discussed in LBCT. In our analysis, we have found the critical relationship T-(t-1)≥t, that is, the maximum number of compromised nodes to tolerate false data injection attacks, *i.e.*, t-1, cannot cooperatively cause the report disruption attacks, thus, we have $T \geq 2t-1$.

From the above analysis, we can see that asymmetric cryptography based signature approaches are more suitable for authentication and en-route data filtering in the IoT scenario. Moreover, such methods should tolerate various node compromise attacks and DoS attacks.

At the same time, the computation and communication overhead should be kept as low as possible.

3. The Proposed Scheme

3.1. Assumptions

We assume that all the sensor nodes in WSNs are deployed uniformly and bootstrapped securely using the scheme proposed in [12] so that the one-hop neighboring sensor nodes can establish pairwise keys and trust relationships to form a network with multi-hop cluster-tree hierarchical topology. Each node establishes and stores a neighbor trust list. We also assume that every event of interest can be detected by multiple, say T (T>1), sensor nodes. Then, the event needs to be reported during which a group of at least t $(T \geq 2t-1)$ nearby legitimate nodes should collaboratively agree on the event that will be forwarded to one or more Internet users. In the scenario, T and t are pre-defined system parameters. This group of neighboring nodes generates and broadcasts the signed report to a lead node which then aggregates the signatures before sending it to one or more Internet users through one or more forwarding nodes. Moreover, we assume that the Internet users are determined by the service provider (SP) based on the service provided by the sensor nodes. The corresponding software code can be preloaded in the sensor nodes prior to deployment. Furthermore, the code can be dynamically updated by using an end-to-end secure communication protocol (referring to [13]).

3.2. Threat Model and Design Goals

An adversary can eavesdrop on all traffic, inject packets, replay older packets and take full control of the compromised nodes to launch false report injection attacks and DoS attacks. In our model, we assume that at most T-t neighboring nodes in an event area can be compromised. Our objective is to design a scheme to detect these attacks for the event report in the IoT scenario. Our scheme should achieve the following goals:

- It should not require the establishment of pre-shared keys between Internet users and sensor nodes.
- It should tolerate node compromises in the WSNs even if the locations of the sensor nodes may not be known.
- It can mitigate the impact of DoS attacks including report disruption attacks and selective forwarding attacks.
- It should keep the overhead of communication and computation as low as possible in the WSNs.

3.3. Preliminaries

3.3.1. ID-based Signature: As discussed above, ECC-based signature (*i.e.*, ECDSA) requires one point multiplication operation to generate a signature and two point multiplication operations to verify a signature. Moreover, authentication of the public key of the signer also requires two point multiplication operations. For an ECC of 160 bites, ECDSA produces a 40-byte signature, resulting in more than an 80-byte message payload (including a 40-byte ECDSA signature and a certificate with at least 46-byte). With the current state of the art technology, the most efficient ID-based signature *(i.e.*, vBNN [14]) needs one point multiplication operation to sign a message and three point multiplication operations to verify

the signature with the length of a signature being 83 bytes. Let's briefly describe the vBNN scheme below.

Given a sensor node ID_i, the SP picks a random number $r_i \in Z_q$, where the multiplicative group $Z_q = [1, \cdots, q-1]$, computes $R_i = r_i P$, where P is a large prime and an elliptic curve $E(F_P)$ is defined over a finite field $F_P = [1, 2, ..., P-1]$. Then, SP calculates $S_i = r_i + xH_1(ID_i \| R_i)$ in which x is the master key of the WSN picked by SP and $H_1 : \{0,1\}^* \times G_1 \to Z_q$, where G_1 is an additive group of the prime order q. R_i and S_i are stored in the sensor node ID_i.

Given a message M, the signer ID_i performs the following steps to sign the message.

1. Choose a random number $y \in Z_q$ and compute $Y = yP$.
2. Compute $h = H_2(ID_i \| M \| R_i \| Y)$ and $z = y + S_i h$, where $H_2 : \{0,1\}^* \to Z_q$.
3. (R_i, h, z) is the digital signature.

The signer then sends (M, R_i, h, z) to the receiver. To verify the message and the signature, the receiver does the following steps.

1. Compute $c = H_1(ID_i \| R_i)$.
2. Check the equation $h = H_2(ID_i \| R_i \| M \| zP - h(R_i + cP_{pub}))$, where $P_{pub} = xP$ is a public parameter.

3.3.2. Verifiable Secret Sharing: Sensor node ID_i generates a secret polynomial $f_{Si}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$, where $a_0, \ldots, a_{t-1}$ are random numbers picked by the sensor node ID_i and the secret key S_i can be picked as $S_i = a_0$. The secret share of S_i for the neighboring node ID_j is thus $C_{Si}^j = f_{Si}(ID_j)$. Then, any t sensor nodes together can reconstruct S_i by using Lagrange interpolation $S_i = \sum_{j=1}^{t} l_j C_{Si}^j$, where $l_j = \prod_{k=1, k \neq j}^{t} \frac{ID_k}{ID_k - ID_j}$ is the Lagrange coefficient. However, it is computationally infeasible if fewer than t sensor nodes try to reconstruct the secret key S_i. All C_{Si}^j must be distributed through the secure communication channels. The sensor node ID_i broadcasts $\varepsilon_0 = g^{a_0}$ and $\varepsilon_n = g^{a_n} \pmod p \, (n = 1, 2, \cdots, t-1)$, and every ID_j can verify the received C_{Si}^j by using the equation $g^{C_{Si}^j} = \prod_{k=0}^{t-1} \varepsilon_k^{ID_j^k} \pmod p$, while ID_i can verify the reconstructed S_i by using the equation $g^{Si} = \varepsilon_0$.

3.4. The Authentication and En-route Data Filtering Scheme

3.4.1. Initialization: During the bootstrapping phase, the lead node in every group distributes the secret share of S_i to all group nodes. Specifically, in ith group, the lead node ID_i generates a secret polynomial $f_{Si}(x)$ and distributes the secret share $f_{Si}(ID_j)$ to every group node ID_j using the shared key between them. Then, ID_i deletes S_i and $f_{Si}(x)$ but stores $f_{Si}(ID_i)$. Therefore, ID_i only needs to be authenticated by any other t-1 group nodes and get t-1 secret shares in order to reconstruct S_i.

3.4.2. Report Generation: When an event occurs, the lead node will prepare a report, say, *E*. To get an agreement on the event from other group nodes, the lead node ID_i broadcasts *E* to all the group nodes and authenticates itself to them. After receiving *E*, a group member will find the difference between the received *E* and what it has sensed. If the difference is within a predefined error range, it will agree on *E* and endorse the signature. These *T* group members including ID_i itself, i.e., ID_j, will generate one random polynomial $f_{yi}^j(x) = a_{j0} + a_{j1}x + a_{j2}x^2 + \cdots + a_{jt-1}x^{t-1}$, in which the share of the random number is $C_{yi}^j(k) = f_{yi}^j(ID_k)(k = 1, 2, \cdots, T)$, and distributes $C_{yi}^j(k)$ to the other sensor nodes ID_k, broadcast $\varepsilon_0 = g^{a_{j0}}$ and $\varepsilon_n = g^{a_{jn}} \pmod p (n = 1, 2, \cdots, t-1)$. Note that the distribution of the secret shares should be protected using the shared keys between the communicating peers. Therefore, each sensor node will receive no less than $m-1(t \le m \le T)$ secret shares which should be verified as discussed in Section 3.3.2.

During the verification phase, a compromised group member may be detected. If ID_j find a corrupted partial secret share sent by a group member, ID_j broadcasts the ID of the compromised group member. If more than *t* members claim that one node has been compromised, each legitimate sensor node can find all compromised group members and no less than *t* legitimate group members. These *m* legitimate sensor nodes use the verified $m-1$ secret shares and its own share to compute the share of y_i, denoted as y_i^j, and $y_i^j = \sum_{k=1}^{m} f_{yi}^k(ID_j)$. $y_i = f_{yi}(0)$ is generated from the polynomial $f_{yi}(x) = \sum_{k=1}^{m} f_{yi}^k(x)$ which is endorsed by these *m* legitimate sensor nodes and. Therefore, no sensor node knows y_i, and any *t* sensor nodes can reconstruct y_i using Lagrange interpolation: $y_i = \sum_{j=1}^{t} l_j y_i^j$.

Each legitimate neighboring node ID_j except the lead node ID_i sends $l_j y_i^j P$ to ID_i which then sums up the received *m* shares to get $Y_i = \sum_{j=1}^{m} l_j y_i^j P$ and broadcasts Y_i along with R_i. Each ID_j including ID_i computes $z_j = l_j y_i^j + l_j C_{si}^j h$, where $h = H_2(ID_i \| E \| R_i \| Y_i)$, and sends z_j to ID_i which then sums up $z = \sum_{j=1}^{m}(l_j y_i^j + l_j C_{si}^j h) = \sum_{j=1}^{m} l_j y_i^j + \sum_{j=1}^{m} l_j C_{si}^j h = y_i + S_i h$. It is possible that some of the neighboring nodes have been compromised during this phase and, thus, may provide the lead node ID_i with incorrect signatures. Therefore, ID_i should verify their authenticity by checking the equation $Y_i = zP - h(R_i + cP_{pub})$ where $c = H_1(ID_i \| R_i)$.

Finally, ID_i broadcasts the final data report (E, R_i, h, z) and assigns multiple upstream nodes in its neighbor trust list to make the report forwarded to the Internet users through multipath routing. In the cases in which the compromised lead node may either not send the final report or transmit a bogus report with a wrong (E, R_i, h, z), it will be detected by all legitimate neighboring nodes. The verification is the same as the en-route filtering operations to be described in Section 3.4.3. In this case, the legitimate neighboring nodes will randomly elect a new lead node among themselves to generate a new threshold-endorsement and send the final report to the Internet users.

3.4.3. En-route Filtering of Data Report: We denote P_f as the en-route verification probability. The forwarding sensor node verifies the signature of a report with the

probability P_f which is a predefined system parameter. As discussed in Section 3.3.1, the verifying intermediate node or the final Internet user checks the equation $h = H_2\left(ID_i \| R_i \| E \| zP - h\left(R_i + cP_{pub}\right)\right)$. The data report will be regarded as authentic and forwarded to multiple upstream nodes in their neighbor trust lists if the verification is successful, otherwise, it will be immediately discarded.

4. Analysis

4.1. Security Analysis

4.1.1. Resilience to Node Compromise Attacks: Our scheme uses the threshold signature generation to sign any event report. The attacker must know the private key S_i and the secret random number y_i to forge the signature of ID_i by compromising at least *t* nodes in the event area. In some cases, the lead node itself may have been compromised, resulting in a higher level of risk. However, our scheme doesn't reveal any C_{Si}^j and y_i^j at any step. Firstly, the initialization phase is secure in which the lead node distributes the shares of S_i within short time after bootstrapping. Secondly, each neighboring node submits $l_j y_i^j P$ rather than y_i^j, making it impossible for the lead node to derive y_i^j from $y_i^j P$ due to the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Thirdly, $z_j = l_j y_i^j + l_j C_{si}^j h$ that is submitted by each neighboring node has two unknown numbers y_i^j and C_{Si}^j, so the lead node cannot derive y_i^j and C_{Si}^j from z_j. Finally, should the lead node change the report with a wrong (E, R_i, h, z) in the final step, it would be detected by the forwarding nodes as well as by all the legitimate neighboring nodes. These nodes can then elect a new lead node to generate a new threshold-endorsement and send the final report to the Internet nodes. In the worst case, even if the attacker can derive the private key S_i by compromising *t* nodes in the event area, it will not affect any other groups.

4.1.2. Mitigation of Report Disruption Attacks: Our scheme leverages verifiable Shamir's secret sharing cryptography described in Section 3.3.2 which has been shown to be secure [15]. In the report generation phase, at least *t* legitimate sensor nodes cooperatively generate the secret random number y_i by exchanging the shares $C_{yi}^j(k) = f_{yi}^j(ID_k)$, which may be disrupted by compromised nodes. For example, an attacker may provide an incorrect share $C_{yi}^j(k)$ to a neighboring node so that it will not get the right share $y_i^j = \sum_{k=1}^{m} f_{yi}^k\left(ID_j\right)$. However, in our scheme, each node will verify the received shares, detect compromised neighboring nodes and broadcast the detection result so that only legitimate shares will be used in the y_i^j and only the shares z_j computed by legitimate neighboring nodes can be used by the lead node. Note, however, that if the attacker only distributes the wrong shares to only some of the legitimate neighboring nodes that are able to detect the wrong shares, based on the detected results broadcast by such neighboring nodes, it is not possible for the legitimate nodes to identify the compromised nodes.

4.1.3. Mitigation of Selective Forwarding Attacks: In our scheme, in order to mitigate selective forwarding attacks, the lead node and the intermediate nodes would forward the

final report (E, R_i, h, z) to multiple upstream nodes that are in their neighbor trust lists to ensure that the report is forwarded to the Internet users through multipath routing. Unless all the forwarding nodes are compromised, the legitimate report will ultimately be delivered to the destinations. However, this solution will incur high communication overhead. In the worst case in which all the upstream nodes of a forwarding node are compromised, another route path should be used by using a secure multi-path routing protocol, such as SPREAD [16], which is out of the scope of this paper.

4.2. Performance Analysis

4.2.1. Computation Overhead: In any scheme, expensive operations are pairing (Pa), point multiplication (Pm) and exponentiation (Exp). In our scheme, each endorsing sensor node needs to do one point multiplication operation to generate $l_j y_i^j P$ and $T \times t$ exponentiation operations including t exponentiation operations to generate $\varepsilon_n (n = 0,1,2,\cdots,t-1)$ and $(T-1) \times t$ exponentiation operations to verify T-1 received shares. In total, the number of computation operations is $T * Pm + T^2 t * Exp$. Meanwhile, each verifying forwarding sensor node needs three point multiplication operations to authenticate the event report. In LBCT, the number of computation operations is $3 * Pa + (T+1) * Pm + 2 * Exp$ without any compromised nodes selected by the lead node and $(2T+1) * Pa + (T+1) * Pm + (T+1) * Exp$ in the worst case, respectively. While each verifying forwarding sensor node needs two pairing operations and one exponentiation operation to authenticate the event report.

4.2.2. Communication Overhead: In our scheme, the *T* sensor nodes have to jointly generate a random number y_i for each report, which contributes most to the communication overhead since the private key S_i can be distributed during the bootstrapping phase. For a share y_i , each sensor node needs to send $T-1$ secret shares to the $T-1$ neighboring nodes and broadcast one promise $\varepsilon_n (n = 0,1,2,\cdots,t-1)$ and one detection result. In the signature generation phase, each legitimate group sensor node sends $l_j y_i^j P$ and z_j to the lead node and the lead node broadcasts Y_i along with R_i . In total, the number of messages to generate a signature of an event report is $(T+t+1)T$ .In LBCT, each endorsing node only needs to send one share $U_{m,n}^i$ to the lead node which should broadcast θ . In total, the number of messages to generate a signature of an event report is *T*.

4.2.3. Comparison Analysis: We employ the similar model to LBCT to analyze and compare energy consumption which is determined by communication overhead as well as computation cost. We assume that the sensor nodes have the same capabilities as those of a standard Crossbow's MICA2 mote which has 8-bit ATmegal 128L clocked at 7.37-MHz microcontroller and complies with the IEEE 802.15.4 standards with data transmission rate of 12.4kbps. According to [4], completing a 160-bit point multiplication operation of ECC, a pairing operation and an exponentiation operation consumes 24.3mJ, 62.73mJ and 2.81mJ, respectively. In addition, MICA2 consumes 52.2 μJ and 19.4 μJ to transmit and to receive one byte, respectively. We assume that the length of the node's ID is 2 bytes, making the lengths of $C_{yi}^j(k)$, ε_n , $l_j y_i^j P$, z_j , Y_i and R_i to be 2*t* bytes, 20*t* bytes, 40 bytes,

20 bytes, 40 bytes and 40 bytes, respectively. The original report is assumed to be 15 bytes, thus allowing us to transmit a report in one data packet. We denote ε as the average number of hops a report travels in the WSNs. For the sake of simplicity, we only consider the single routing path, thus, both schemes involve εP_f en-route filtering operations. In the analysis, we specify (t, T) to be (2, 3), (3, 5), (4, 7), (5, 9) and (6, 11), respectively due to the relationship between t and T discussed in Section 2.4.

Figure 2 shows the energy consumption for various ε when $P_f = 0.2$ in the condition that the number of compromised nodes in the event group is $T - t$. We can see from the figure that the energy consumption in our scheme is lower than that in LBCT for (2, 3), (3, 5), (4, 7), (5, 9) and the difference narrows as T increases. However, our scheme will consume more energy than LBCT when (t, T) is larger than (6, 11). In addition, ε increases one hop, the increased energy consumption which is about 15mJ in our scheme is fewer than that in LBCT which is more than 25mJ. That is because the energy consumption of computation in our scheme incurring O(t) cost of point multiplication and O(t^2T) cost of exponentiation for report generation and three point multiplication operations for report en-route verification is lower than that in LBCT incurring O(T) cost of pairing and O(t) cost of point multiplication as well as O(T) cost of exponentiation for report generation and two pairing operations and one exponentiation operation for report en-route verification. However, the energy consumption of communication in our scheme which generates O(t^2,T) communication cost is higher than that in LBCT which only generates O(t,T) communication cost.

Figure 3 shows the energy consumption for various P_f when $\varepsilon = 10$ in the condition that the number of compromised nodes in the event group is $T - t$. The difference of energy consumption gets higher as P_f increases. This is because one filtering operation requires two pairings and one exponentiation in LBCT which incurs more cost of computation, about 128mJ, than three point multiplications, about 72 mJ, of one filtering operation in our scheme.

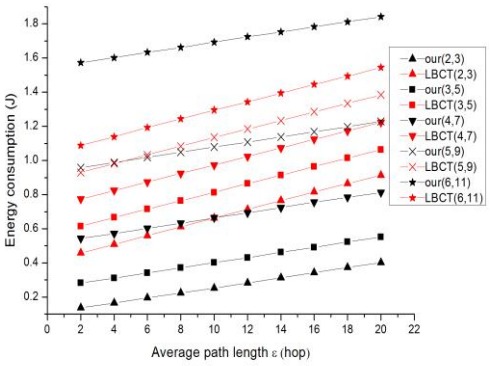

Figure 2. Energy Consumption for Various ε when $P_f = 0.2$

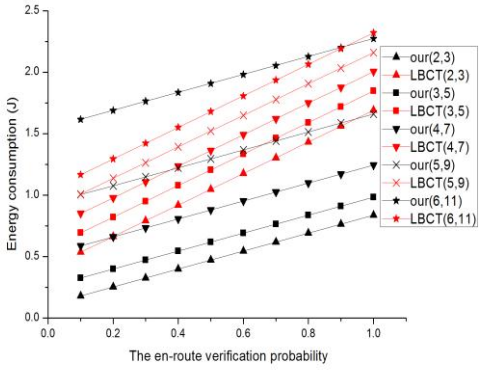

Figure 3. Energy Consumption for Various P_f when $\varepsilon = 10$

5. Conclusion

In this paper, we proposed an authentication and en-route filtering scheme for WSNs in the IoT scenario in which the verifiable secret sharing cryptography is used for the distribution of the shares to multiple collective sensor nodes based on the most efficient ID-based signature

scheme. As long as the adversary doesn't compromise more than *T-t* group nodes in an event area, any event report can be collectively generated with a digital signature attached and forwarded through multipath routing to multiple Internet nodes. Analysis on the proposed scheme showed that our scheme can defend effectively against node compromised attacks and DoS attacks. Quantitative analysis to compare our scheme to LBCT has also been performed in terms of energy consumption, which showed that our scheme outperforms LBCT when fewer numbers of nodes and more numbers of compromised nodes of a group exist in the event area. In the future, we will conduct more experiment in real network setting to verify the results and to further improve the performance in terms of latency in our scheme.

Acknowledgments

The work in this paper has been supported by funding from National Natural Science Foundation of China (61272500) and from Beijing Education Commission Science and Technology Fund (KM201010005027).

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, **(2007)**.
[2] G. Montenegro, N. Kushalnagar and J. Hui, "Transmission of IPv6 packets over IEEE 802.15.4 networks", IETF RFC 4944, **(2007)**.
[3] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-based compromised-tolerant security mechanisms for wireless sensor networks", IEEE Journal on Selected Area in Communications, vol. 24, no. 2, **(2006)**.
[4] L. B. Oliveira, A. Kansal, B. Priyantha and M. Goraczko, "Secure-TWS: Authenticating node to multi-user communication in shared sensor networks", Proceedings of the 8th International Conference on Information Processing in Sensor Networks, **(2009)** April 13-16; San Francisco, California, USA.
[5] R. Yasmin, E. Ritter and G. Wang, "An authentication framework for wireless sensor networks using identity-based signatures", Proceedings of the 10th IEEE International Conference on Computer and Information Technology, **(2010)** June 29-July 1; Bradford, UK.
[6] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks", Proceedings of IEEE INFOCOM, **(2004)** March 7-11; Hong Kong, China.
[7] S. Zhu, S. Setia, S. Jajodia and P. Ning, "An interleaved hop-by-Hop authentication scheme for filtering of injected false data in sensor networks", Proceedings of IEEE Symposium on Security and Privacy, **(2004)** May 9-12; Berkeley, CA, USA.
[8] Q. Sun and M. Wu, "A double key-sharing based false data filtering scheme in Wireless Sensor Networks", Proceedings of International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, **(2011)** November 16-18; Changsha, China.
[9] H. Yang, F. Ye, Y. Yuan, S. Lu and W. Arbaugh, "Toward resilient security in wireless sensor networks", Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing, **(2005)** May 25-28; Urbana-Champaign, IL, USA.
[10] K. Ren, W. Lou and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks", Proceedings of IEEE INFOCOM, **(2006)** April 23-29; Barcelona, Spain.
[11] H. Wang and Q. Li, "Achieving robust message authentication in sensor networks: a public-key based approach", Wireless Networks, vol. 16, no. 4, **(2010)**.
[12] H. Yu and J. He, "Trust-based mutual authentication for bootstrapping in 6LoWPAN", Journal of Communications, vol. 7, no. 8, **(2012)**.
[13] H. Yu, J. He, T. Zhang, P. Xiao and Y. Zhang, "Enabling end-to-end secure communication between wireless sensor networks and the Internet", World Wide Web Journal, in publishing.
[14] X. Cao, W. Kou, X. Zeng and L. Dang, "Identity-based anonymous remote authentication for value-added services in mobile networks", IEEE Trans. on Vehicular Technology, vol. 58, no. 7, **(2009)**.
[15] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", Proceedings of the 28th Annual FOCS, **(1987)** October 12-14; Los Angeles, CA, USA.
[16] W. Lou, W. Liu and Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks", Proceedings of IEEE INFOCOM, **(2004)** March 7-11; Hong Kong, China.

Authors

Hong Yu received her Master's degree in Computer Science and Technology 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 and she has published several research papers in scholarly journals and international conferences in the above research areas.

Jingsha He received his B.S. degree in Computer Science from Xi'an Jiaotong University in Xi'an, China and his M.S. and Ph.D. degrees in Computer Engineering from University of Maryland at College Park in U.S.A. He is currently a professor in the School of Software Engineering at Beijing University of Technology in Beijing, China. Professor He's research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security and he has published over 170 research papers in scholarly journals and international conferences and has been granted nearly 30 patents in the United States and in China.