Long Duration Broadcast Authentication for Wireless Sensor Networks

Yongsheng Liu, Jie Li,
Graduate School of System and Information Engineering
University of Tsukuba
Tsukuba Science City, 305-8573, Japan
liuyongsheng@osdp.cs.tsukuba.ac.jp, lijie@cs.tsukuba.ac.jp,

Minyi Guo
Shanghai Key Lab of Scalable Computing and Systems
Department of Computer Science and Engineering
Shanghai Jiao Tong University, Shanghai, P.R. China
guo-my@cs.sjtu.edu.cn

***Abstract*—In the resource constrained Wireless Sensor Networks (WSNs), the broadcast authentication is widely fulfilled by the emerging delayed authentication technique. The one level backward one-way key chain in the delayed authentication technique limits heavily the duration of the broadcast authentication. In this paper, we propose a long duration broadcast authentication scheme for WSNs. The proposed scheme uses a novel hierarchical key chain to extend the duration of broadcast authentication to be as long as the whole lifetime of WSNs. Moreover, the overhead of the proposed scheme is significantly reduced compared to that with one level key chain. Extensive experimental results show that the novel hierarchical key chain fully outperforms the one level key chain in terms of memory and computation.**

I. Introduction

Wireless Sensor Networks (WSNs) have been drawing considerable attention in recent years due to its increasing applications in environmental monitoring, target tracking, object detection, etc. A WSN consists of one or more base stations and hundreds of sensor nodes [1]. Base stations serve as gateways between the Internet users and sensor nodes. Sensor nodes equipped with the microcontroller, the radio frequency transceivers and sensing units are scattered into a specified area to monitor physical conditions. Since powered by batteries, sensor nodes have limited energy supply, which constrains their computation, communication and memory capabilities.

In WSNs, the broadcast transmission is one of the fundamental communication primitives. The base station may conduct network queries [2] and distribute code images [3] by broadcast. The sensor node may broadcast packets to discover neighbors or exchange the routing information. The broadcast packets are appeal to an adversary. The adversary may intercept the broadcast packet, modify its content and rebroadcast it. To resist the attacks, broadcast packets should be authenticated.

In the resource constrained WSNs, the broadcast authentication is widely fulfilled by the emerging delayed authentication technique (e.g., [4] [5] [6] [7]). It achieves asymmetry by delayed disclosure of secret keys, and utilizes Message Authentication Codes (MACs) to authenticate broadcast packets. The representative of the delayed authentication technique is μTESLA [4]. In μTESLA, the sender generates an one level backward one-way key chain for broadcast authentication. The one level key chain is generated by selecting the last key K_n and successively applying one-way function F to K_n in order to produce other keys. The first key K_0 is called the commitment of the key chain. Each key in the key chain except the commitment is associated with one time interval. Before broadcast authentication, the sender unicasts initial parameters including the commitment, starting time, and the length of one time interval to each receiver in an authenticated manner. In the broadcast authentication, the secret key belonging to current time interval, say K_i, is used to compute MACs for broadcast packets. After broadcast packets reaching receivers, K_i is disclosed to receivers. Receivers first authenticate K_i by verifying $K_0 = F^i(K_i)$. With the authenticated K_i, receivers authenticate broadcast packets by verifying their MACs.

The backward one level key chain, however, limits heavily the duration of the broadcast authentication. The long key chain is beyond the memory capability of sensor nodes and gives rise to high computation overhead. The long time interval for each secret key incurs overflow of receivers when buffering broadcast packets. Thus, if the broadcast authentication lasts for a long duration, the initial parameters need to be updated successively. The update of the initial parameters, which is accomplished by the unicast transmission, introduces high communication overhead. To reduce the high communication overhead, Liu et al. [5] propose Multilevel μTESLA to replace unicast with broadcast to update the initial parameters.

In this paper, we propose a long duration broadcast authentication scheme for WSNs. The proposed scheme uses a novel hierarchical key chain to extend the duration of broadcast authentication to be as long as the whole lifetime of WSNs. Moreover, the overhead of the proposed scheme is significantly reduced compared to that with one level key chain. Extensive experimental results show that the novel hierarchical key chain fully outperforms the one level key chain in terms of memory and computation. The main contributions of this paper are summarized as follows.

- A novel hierarchical key chain for the delayed authentication technique is proposed to extend its duration.
- A long duration broadcast authentication scheme using the hierarchical key chain is presented.
- Extensive experiments are carried out to evaluate the hierarchical key chain.

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

II. System Description

We consider a WSN consisting of one or more base stations and hundreds of sensor nodes. The base station is endowed with powerful capabilities or the same as a sensor node. A sensor node is resource constrained and vulnerable to adversaries. In the WSN, adversaries may launch both the external attacks and the internal attacks. In the external attacks, adversaries could modify broadcast packets, inject broadcast packets, and replay previously intercepted packets. In the internal attacks, the adversaries are able to compromise some sensor nodes and obtain the sensitive information (e.g., secret keys).

We consider the scenario that one sender broadcasts packets to many receivers. The sender may be the base station or a sensor node. The sender is denoted by s. Let h denote the levels in the hierarchical key chain. The initial parameters for sender s include the keys K_0, the n-to-n functions NF_1, NF_2, ..., NF_{h-1}, NF_{12}, NF_{23}, ..., $NF_{(h-2)(h-1)}$, the one-way functions F_h and $F_{(h-1)h}$, the disclosure delay δ, and the duration of one time interval T. Corresponding to sender s, there are c receivers in total, denoted by a set $R^s = \{r_i^s, 1 \leq i \leq c\}$. Receivers are sensor nodes. The initial parameters for one receiver are the key K_0, the n-to-n functions NF_1, NF_2, ..., NF_{h-1}, NF_{12}, NF_{23}, ..., $NF_{(h-2)(h-1)}$, the one-way functions F_h and $F_{(h-1)h0}$, the disclosure delay δ, and the duration of one time interval T. Note that the difference in the initial parameters is $F_{(h-1)h0}$ at the receiver side and $F_{(h-1)h}$ at the sender side. The key K_0 is of length n. The n-to-n function and the one-way function shown in definition 1 and 2, respectively, map a string of length n to another of length n. Thus, all keys are restricted to length n. The disclosure delay δ is the number of time intervals, after which sender s discloses the secret key. A time interval is denoted by I_i, $i = 1, 2, 3, ...$, the duration of which is T. As stated in μTESLA, the initial parameters for receivers are distributed in an authenticated manner before broadcast authentication, and the sender and receivers are loosely time synchronized.

Defintion 1 (n-to-n function NF)**.** *A n-to-n function NF maps a string of length n to a different string of length n.*

Definition 2 (one-way function F)**.** *A n-to-n function F is called one-way if there is an efficient algorithm to compute $F(x)$ on input x, whereas any feasible algorithm that tries to find a preimage of $F(x)$ may succeed only with negligible probability.*

III. Proposed Long Duration Broadcast Authentication Scheme

The proposed scheme employs the novel hierarchical key chain to authenticate broadcast packets. At the sender side, the highest level of the hierarchical key chain is generated forward from the key K_0 and the lower level starts from the key in the higher level. The keys in the lowest level that is generated backward act as the secret keys to produce MACs of broadcast packets. By using a different one-way function, the receiver can only generate the the first key of the key chain in the lowest level, called the commitment to the key chain.

This section is presented in three parts. The first part introduces the hierarchical key chain at the sender side and the receiver side, respectively. The second part describes the generation of the broadcast packets. The third part describes the authentication of the broadcast packets.

A. Hierarchical Key Chain

Note that the hierarchial key chain at sender side is different from that at the receiver side. We introduce the hierarchical key chains for the sender and receivers as follows.

1) **Hierarchical Key Chain at the Sender Side:** The one level backward one-way key chain has limited secret keys. The problem is circumvented by the infinite backward one-way key chains in the hierarchical key chain.

Specifically, sender s generates the hierarchical key chain as follows.

The first level starts from the key K_0. By applying the function NF_1 successively to K_0, keys in the first level is generated, as shown in equation (1). It is worth noting that since the first level is generated forwards, its length is infinite.

$$K_{x_1} = NF_1^{x_1}(K_0), x_1 = 1, 2, ... \tag{1}$$

Other levels except the h-th level are generated in the following way. The key chain in the i-th level, $2 \leq i \leq h-1$, for instance, starts from the key $K_{x_1...x_{i-1}}$ in the $(i-1)$-th level, as shown in equation (2) where $K_{x_1...x_{i-1}1}$ stands for the first key of the key chain in the i-th level. By applying the function NF_i successively to $K_{x_1...x_{i-1}1}$, other keys of the key chain in the i-th level are generated, as shown in equation (3) where n_i refers to the number of keys in the key chain. Unlike that there are infinite keys in the first level, the number of keys in one key chain in the i-th level key chain is limited to n_i.

$$K_{x_1...x_{i-1}1} = NF_{(i-1)i}(K_{x_1...x_{i-1}}) \tag{2}$$

$$K_{x_1...x_{i-1}x_i} = NF_i^{x_i-1}(K_{x_1...x_{i-1}1}), 2 \leq x_i \leq n_i \tag{3}$$

The key chain in the h-th level starts from the key in the $(h-1)$-th level. The difference is that the last key of the key chain in the h-th level is generated first with the one-way function $F_{(h-1)h}$, as shown in equation (4) where n_h refers to the number of keys in the key chain in the h-th level. By applying the one-way function F_h successively to $K_{x_1...x_{h-1}(n_h-1)}$, other keys in the key chain in the h-th level are generated, as shown in equation (5). Hence, the key chain in the h-th level is generated backwards. Because F_h is the one-way function, it is infeasible for an adversary to figure out the key $K_{x_1...x_{h-1}(x_h+1)}$ from the key $K_{x_1...x_{h-1}x_h}$. Note that the first key of the key chain in the h-th level is $K_{x_1...x_{h-1}0}$. Conventionally, $K_{x_1...x_{h-1}0}$ is called the commitment to the key chain. Other keys in same key chain are called the secret keys since they are used to produce MACs of broadcast packets.

$$K_{x_1...x_{h-1}(n_h-1)} = F_{(h-1)h}(K_{x_1...x_{h-1}}) \tag{4}$$

$$K_{x_1...x_{h-1}x_h} = F_h^{n_h-x_h-1}(K_{x_1...x_{h-1}(n_h-1)}), 0 \leq x_h \leq n_h-2 \tag{5}$$

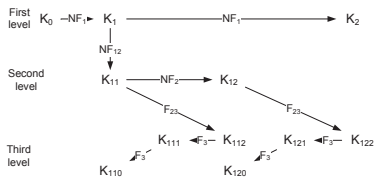

Fig. 1. An example of the hierarchical key chain at the sender side

At this point, we finish generating the hierarchical key chain at the sender side. Fig. 1 illustrates the hierarchical key chain with three levels at the sender side, where each key chain in the second level has two keys and each key chain in the third level has three keys.

Although the length of the key chain in the h-th level is limited, in total there are infinite secret keys in the hierarchical key chain.

Lemma 1. *The number of the secret keys (keys in the h-th level) in the hierarchical key chain at the sender side is infinite.*

Proof: There are infinite keys in the first level. Because each key chain in the second level originates from one key in the first level, the number of key chains in the second level is infinite. Since each key chain in the second level contains n_2 keys, the number of key chains in the third level is infinite. This continues to the h-th level. The number of key chains in the h-th level is infinite. Since each key chain in the h-th level contains $(n_h - 1)$ secret keys, the number of secret keys in the hierarchical key chain is infinite. ■

2) **Hierarchical Key Chain at the Receiver Side:** At the receiver side, we hide the secret keys and maintain the commitments in the lowest level. This is fulfilled by the selected one-way function between the lowest level and the penultimate level.

In detail, the receiver in R^s generates the hierarchical key chain as follows.

The first level to the $(h-1)$-th level are generated in the same way as at the sender side.

Each key chain in the h-th level is restricted to the commitment. This is done by applying the function $F_{(h-1)h0}$ to the key in the $(h-1)$-th level. The function $F_{(h-1)h0}$ is a composition of one-way functions, as shown in equation (6) where n_h represents the number of keys in the key chain in the h-th level. Due to the composition of one-way functions, $F_{(h-1)h0}$ retains the properties of the one-way function. According to equation (6), it is apparent that the output of $F_{(h-1)h0}$ on the input of the key $K_{x_1 \ldots x_{h-1}}$ in the $(h-1)$-th level is the commitment $K_{x_1 \ldots xh-10}$, as shown in equation (7).

$$F_{(h-1)h0} = F_h^{n_h - 1} \circ F_{(h-1)h} \tag{6}$$

$$K_{x_1 \ldots x_{h-1}0} = F_{(h-1)h0}(K_{x_1 \ldots x_{h-1}}) \tag{7}$$

At this point, we finish generating the hierarchical key chain at the receiver side. Fig. 2 illustrates the hierarchical key chain with three levels at the receiver side, where each key chain in the second level contains two keys.

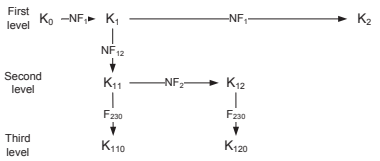

Fig. 2. An example of the hierarchical key chain at the receiver side

It is worth noting that the receiver cannot deduce the secret keys as shown in the lemma below.

Lemma 2. *The secret keys cannot be figured out with the initial parameters at the receiver side.*

Proof: With the initial parameters at the receiver side, there are only two ways to deduce the secret keys. One is from the commitment, and the other is from the key in the $(h-1)$-th level, as shown in Fig. 1.

Because the key chain in the h-th level is generated backward with the one-way function, it is infeasible to deduce secret keys from its commitment.

Deducing the secret keys from the keys in the $(h-1)$-th level needs the one-way function $F_{(h-1)h}$. The expression of $F_{(h-1)h}$ is shown in equation (8).

$$F_{(h-1)h} = (F_h^{n_h})^{-1} \circ F_{(h-1)h0} \tag{8}$$

Equation (8) deals with computing the inverse of the one-way function F_h, which is infeasible. Thus, $F_{(h-1)h}$ cannot be figured out.

Summarily, the secret keys cannot be figured out with the initial parameters at the receiver side. ■

Since there are infinite key chains in the h-th level, there are infinite commitments at the receiver side.

Lemma 3. *The number of commitments in the hierarchical key chain at the receiver side is infinite.*

B. Generating Broadcast Packets

Sender s associates each secret key with one time interval. In the associated time interval, the secret key is used to produce MACs of broadcast packets. According to lemma 1, there are infinite secret keys in the hierarchical key chain at the sender side. Thus, the hierarchical key chain can cover the lifetime of sender s as shown in the theorem below.

Theorem 4. *The hierarchical key chain keeps usable in the whole lifetime of the sender when secret keys are associated with time intervals.*

Although there are infinite secret keys, sender s only needs to buffer the latest key in the first level since the hierarchical key chain offers an efficient way to compute the secret key belonging to the current time interval. Recall that each secret key is associated with one time interval and each key chain in the h-th level contains $(n_h - 1)$ secret keys. Thus, one key in the $(h-1)$-th level spans $(n_h - 1)$ time intervals. Likewise, the key in the $(h-2)$-th level spans $(n_h - 1)n_{h-1}$ time intervals. Therefore, each key in the first level spans $(n_h - 1)\prod_{l=2}^{(h-1)} n_l$ time intervals. That means if the duration of two consecutive

broadcast packets is equal to $(n_h-1)\prod_{l=2}^{(h-1)} n_l$ time intervals, one computation of the n-to-n function on the buffered key is enough to step in the current time interval. In contrast to that, it gives rise to $(n_h-1)\prod_{l=2}^{(h-1)} n_l$ computations of the one-way function for the one level key chain. In general, suppose the buffered key in the first level is K_p and current time interval is I_r. Computing the secret key belonging to time interval I_r from key K_p is conducted according to Algorithm 1. The overhead is summarized in Theorem 5.

Theorem 5. *At the sender side, the memory overhead of the hierarchical key chain is $O(1)$, and the computation overhead to obtain the secret key belonging to time interval I_r from key K_p is $O(\lfloor r/((n_h-1)\prod_{l=2}^{(h-1)} n_l)\rfloor + \sum_{l=2}^{h} n_l - p)$.*

Algorithm 1 Computing the secret key at the sender side

1: $j = r$
2: $K_t = K_p$
3: **for** $i = 1 \rightarrow h-1$ **do**
4: Compute the index of the key in the i-th level corresponding to I_r by $x_i = \lfloor j/((n_h-1)\prod_{l=i+1}^{(h-1)} n_l)\rfloor$
5: **if** i==1 **then**
6: Compute the key by $K_t = NF_i^{x_i-p}(K_t)$
7: **else**
8: Compute the key by $K_t = NF_i^{x_i-1} \circ NF_{(i-1)i}(K_t)$
9: **end if**
10: Compute $j = j \mod ((n_h-1)\prod_{l=i+1}^{(h-1)} n_l)$
11: **end for**
12: Compute the index of the key in h-th level by $x_h = n_h - j$
13: Compute the secret key for time interval I_r by $K_{x_1 \ldots x_{h-1} x_h} = F_h^{n_h - x_h} \circ F_{(h-1)h}(K_t)$

After having obtained the secret key $K_{x_1 \ldots x_{h-1} x_h}$ belonging to time interval I_r, sender s computes MACs of broadcast packets. In time interval $I_{(r+\delta)}$ when sender s is assured that broadcast packets plus their MACs have reached all receivers, sender s discloses secret key $K_{x_1 \ldots x_{h-1} x_h}$ to receivers.

C. Authenticating Broadcast Packets

The commitment at the receiver side is also associated with time intervals. Since the key chain in the h-level at the sender side includes (n_h-1) secret keys, each commitment at the receiver side is associated with (n_h-1) time intervals. According to lemma 3 that there are infinite commitments, the hierarchical key chain can cover the lifetime of the receiver as shown in Theorem 6.

Theorem 6. *The hierarchical key chain keeps usable in the whole lifetime of the receiver when commitments are associated with time intervals.*

After a broadcast packet arrives at the receiver in R^s, the receiver first checks whether the secret key for the broadcast packet is disclosed or not. If the secret key has been disclosed, an adversary can forge the broadcast packet with a valid MAC. The check is conducted by judging whether the arrival time interval of the broadcast packet is before the time interval when sender s discloses the secret key. Recall that we assume that receivers in R^s are loosely time synchronized with sender s. If the secret key has not been disclosed yet, the receiver buffers the packet. Otherwise, the receiver drops it.

When the disclosed secret key $K_{x_1 \ldots x_{h-1} x_h}$ arrives, the receiver authenticates it by the commitment that is computed by the receiver itself. The hierarchical key chain provides an efficient way to compute the commitment, which is similar to computing secret keys at the sender side shown in algorithm 1. Thus, we obtain the corresponding memory overhead and computation overhead as summarized in Theorem 7.

Theorem 7. *At the receiver side, the memory overhead of the hierarchical key chain is $O(1)$, and the computation overhead to obtain the commitment associated with time interval I_r from key K_p is $O(\lfloor r/((n_h-1)\prod_{l=2}^{(h-1)} n_l)\rfloor + \sum_{l=2}^{h-1} n_l - p)$.*

As soon as the commitment $K_{x_1 \ldots x_{h-1} 0}$ is obtained, the receiver authenticates the disclosed key $K_{x_1 \ldots x_{h-1} x_h}$ by equation (9). Because the number of keys in the key chain in the h-th level is limited to n_h, the authentication overhead is bounded by $O(n_h)$ as shown in lemma 8. Whereas, the authentication overhead of the one level key chain equals the distance in time intervals between the disclosed key and the commitment or the recently authenticated secret key. That means if the duration of two consecutive broadcast packets is large, the authentication overhead will be very high.

$$K_{x_1 \ldots x_{h-1} 0} = F_h^{x_h}(K_{x_1 \ldots x_{h-1} x_h}) \tag{9}$$

Lemma 8. *The computation overhead to authenticate one disclosed key is $O(n_h)$*

With the authenticated secret key, the receiver authenticates the broadcast packet by verifying its MAC.

IV. Experiments and Results

The experiments concentrate on the computation overhead and memory overhead of the hierarchical key chain.

A. Implementation

The experiments are conducted on the testbed consisting of TelosB sensor nodes [8]. The program is implemented by NesC on TinyOS 2.1. The length of each key is 20 bytes. The one-way functions and the n-to-n functions are implemented by SHA-1, which has been used previously (e.g., [9]).

We compare four types of key chains: one level key chain, the hierarchical key chain with two levels where the key chain in the second level contains 60 keys (denoted by HKC2), the hierarchical key chain with three levels where the key chain in the second level and third level contains 60 keys (denoted by HKC3-1), the hierarchical key chain with three levels where the key chain in the second level and third level contains 30 keys (denoted by HKC3-2). The evaluation of the key chain deals with computing the secret key from the buffered key. Since each secret key is associated with one time interval, the distance in time interval between the computed secret key and the buffered key is referred to as the covered duration. All experimental results are averaged over 10 runs.

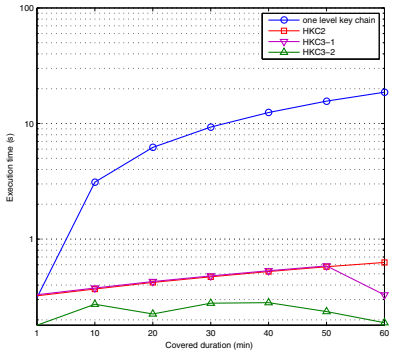

Fig. 3. Execution time with respect to the covered duration

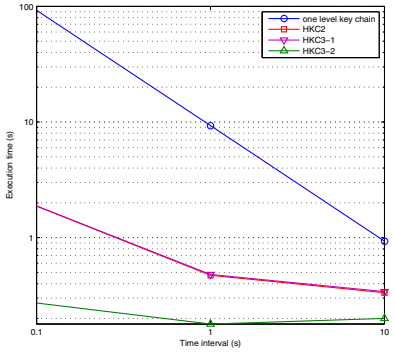

Fig. 4. Execution time with respect to the time interval

B. Experimental Results

The computation overhead of the key chains is measured by the execution time to calculate the secret key from the buffered key. Fig. 3 illustrates the execution time with respect to the covered duration, in which the time interval is set to 1 s. To show more details about the hierarchical key chain, the execution time axis increases logarithmically. It can be seen that the execution time of the one level key chain is proportional to the covered duration. Whereas, the maximum execution time of the hierarchical key chain is 0.6 s. Specifically, the execution time of HKC2 increases monotonously with the duration increasing. The reason is that the increase of the covered duration leads to the advance in the first level. The drastic decrease of HKC3-1 when the covered duration is 60 min results from one forward step in the first level. Fig. 4 shows the execution time with respect to the time interval, in which the covered duration is 30 min. The execution time axis increases logarithmically. That the time interval decreases from 10 s to 0.1 s results in that the execution time of the one level key chain increases from 1 s to 100 s. The effect is not obvious for the hierarchical key chain. This is because the higher level in the hierarchical key chain counteracts effectively the computation overhead caused by the small time interval. The execution time of HKC2 equals HKC3-1 since one key in the first level spans 60 min.

Fig. 5 shows the memory overhead of the one level key chain with respect to the covered duration. The memory overhead is proportional to the covered duration no matter what the time interval is. When the covered duration is 60 min, the memory overhead is beyond the RAM capability of the TelosB sensor node .

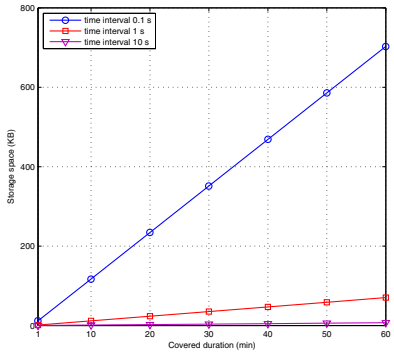

Fig. 5. Memory overhead of the one level key chain

V. Conclusion

The one level backward one-way key chain in the delayed authentication technique limits heavily the duration of the broadcast authentication. In this paper, we propose a long duration broadcast authentication scheme for WSNs. The proposed scheme uses a novel hierarchical key chain to extend the duration of broadcast authentication to be as long as the whole lifetime of WSNs. Moreover, the overhead of the proposed scheme is significantly reduced. Extensive experimental results show that the novel hierarchical key chain fully outperforms the one level key chain in terms of memory and computation.

Acknowledgment

This work has been partially supported by Grand-in-Aid for Scientific Research from Japan Society for Promotion of Science (JSPS), Research Collaboration Grant from NII of Japan, and 863 program 2011AA01A202 and NSFC (Grant No. 60725208, 61003012).

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 2–16, 2003.

[3] J. W. Hui and D. Culler, "The dynamic behavior of a data dissemination protocol for network programming at scale," in *ACM SenSys*, 2004, pp. 81–94.

[4] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[5] D. Liu and P. Ning, "Multilevel μTESLA: Broadcast authentication for distributed sensor networks," *ACM Transactions on Embeded Computing Systems*, vol. 3, pp. 800–836, 2004.

[6] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, pp. 1–35, 2008.

[7] T. Kwon and J. Hong, "Secure and efficient broadcast authentication in wireless sensor networks," *IEEE Transactions on Computers*, vol. 59, no. 8, pp. 1120–1133, 2010.

[8] J. Polastre, R. Szewczyk, and D. Culler, "Telos: enabling ultra-low power wireless research," in *IEEE IPSN*, 2005, pp. 364–369.

[9] A. Liu, P. Ning, and C. Wang, "Lightweight remote image management for secure code dissemination in wireless sensor networks," in *IEEE INFOCOM*, 2009, pp. 1242–1250.