Journal of Computer Science and Information Technology
December 2014, Vol. 2, No. 3 & 4, pp. 107-125
ISSN: 2334-2366 (Print), 2334-2374 (Online)

Published by American Research Institute for Policy Development
DOI: 10.15640/jcsit.v2n3-4a6
URL: http://dx.doi.org/10.15640/jcsit.v2n3-4a6

Comprehensive Analysis of Broadcast Authentication protocols in Wireless Sensor Networks[1]

Masoum Farahmandian[2], Mohammad Masdari[3] & Vahid Farahmandian[4]

Abstract

Wireless sensor networks (WSNs) due to law costs and easy communication are used in different environments for surveillance activities. One the most important issues raised in these networks is the usage of a good broadcast authentication mechanism. This mechanism helps to provide the security of these networks efficiently. User authentication is a crucial service in wireless sensor networks that is becoming increasingly common in WSNs because wireless sensor nodes are typically deployed in an unattended environment, leaving them open to possible hostile network attack. Because wireless sensor nodes are limited in computing power, data storage and communication capabilities, any user authentication protocol must be designed to operate efficiently in a resource constrained environment.A broadcast authentication mechanism is important in wireless sensor networks. Researchers have provided various authentication mechanisms– which have their own advantages and disadvantages– in these networks. In this paper we analyze and review some popular authentication schemes which are recently proposed for WSNs.

Keywords: Wireless sensor networks, broadcast, authentication, security, protocol

1. Introduction

Wireless sensor networks (WSNs) have enabled data gathering from a vast geographical region and present unprecedented opportunities for a wide range of tracking and monitoring applications from both the civilian and military domains [1, 2].

[1] This study is sponsored by American Research Institute for Policy Development.
[2] Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran. Email: farahmandian@umsu.ac.ir
[3] Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran. Email: m.masdari@Iaurmia.ac.ir
[4] Faculty of Medicine, Tarbiat Modares University,Tehran, Iran. Email: v.farahmandian@modares.ac.ir

In these applications, WSNs are expected to process, store, and provide the sensed data to the network users upon their demands [3]. As the most common communication paradigm, the network users are expected to issue the queries to the network to obtain the information of their interest. Furthermore, in wireless sensor and actuator networks [4], network users may need to issue their commands to the network (probably based on the information that they received from the network). In both cases, there could be a large number of users in the WSNs, which might be either mobile or static, and the users may use their mobile clients to query or command the sensor nodes from anywhere in the WSN. Obviously, broadcast/ multicast1 operations are fundamental to the realization of these network functions. Hence, it is also highly important to ensure broadcast authentication for security purposes [5].

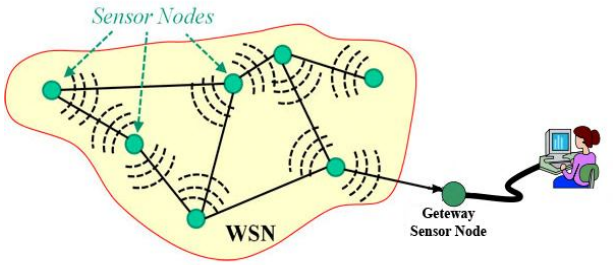

Figure 1: Wireless Sensor Network Scenario

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation, and anti-playback. Finally, all communications need to be kept private so that eavesdroppers cannot intercept study and analyze, and devise counter measures in order to circumvent the purposes of the sensor network [6].

Authentication is a crucial service in wireless sensor networks (WSNs) that is becoming increasingly common in WSNs because wireless sensor nodes are typically deployed in an unattended environment, leaving them open to possible hostile network attack Because wireless sensor nodes are limited in computing power, data storage and communication capabilities, any user authentication protocol must be designed to operate efficiently in a resource constrained environment [7].

In point-to-point authentication, authentication can be achieved through purely symmetric means: the sender and receiver would share a secret key used to compute a cryptographic message authentication code (MAC) over each message [8, 9]. When a message with a valid MAC is received, the receiver can be assured that the message originated from the sender. Researchers showed that MACs can be efficiently implemented on resource-constrained sensor network nodes [10], and find that computing a MAC function requires on the order of 1ms on the computation-constrained Berkeley mote platform [11, 12].

Broadcast authentication is a basic and important security mechanism in a WSN because broadcast is a natural communication method in a wireless environment. When base stations want to send commands to thousands of sensor nodes, broadcasting is a much more efficient method than unicasting to each node individually [13].

In this paper we analyze some popular Authentication schemes which are proposed for WSNs in the literature.

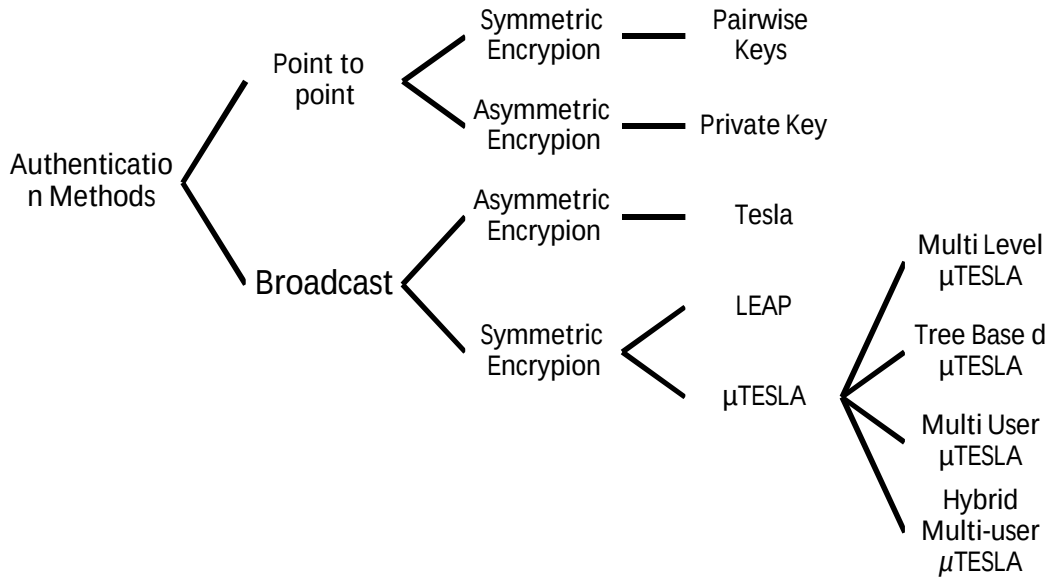

Figure 2: Authentication Methods

2. Broadcast Authentication

A message authentication code (MAC) is an authentication tag derived by applying an authentication scheme and a secret key to a message. MAC is an efficient symmetric cryptographic primitive for two-party authentication; however, MAC is not suitable for broadcast communication without additional modification. Because the sender and its receivers share the same secret key, any one of the receivers can impersonate the sender and forge messages to other receivers. That is, both sender and receivers can sign messages. This problem stems from the symmetric property of MAC [13].

Therefore, to achieve authenticated broadcasts, it is necessary to establish an asymmetric mechanism in which only the sender can sign messages, and the receivers can only verify messages [13].

However, asymmetric cryptographic mechanisms like RSA digital signatures are significantly more computationally expensive than symmetric ones. It is impractical to use them in a resource limited sensor network. A possible approach is to use efficient symmetric primitives as a tool to design a scheme with asymmetric properties [13].

The TESLA [14] protocol provides efficient broadcast authentication over the Internet which can scale to millions of users, tolerate packet loss, and support real time applications [15].Currently, TESLA is in the process of being standardized in the MSEC working group of the IETF for multicast authentication [16].

TESLA presents quite a few advantages over other approaches. For example, sensor nodes only need to compute light-weight hash values for verification in TESLA. However, the least computation demand is at the expense that sensor nodes should buffer received broadcast messages until a later time when they can be verified. In a large sensor network, such a requirement can limit its application, because the verification delay may be too large for sensor nodes to allocate enough buffering storage or may reduce the timeliness of the broadcast information [17].

Table1: Properties of Broadcast Authentication

Desired property	Approach property
Resistance to node compromise	Network-wide key
Low computation overhead	Digital signatures
Low communication overhead	One-time signatures
Robustness to packet loss	HORS + chaining of public keys
Immediate authentication	μTESLA
Messages sent at irregular times	RPT, described in Section 3.3
High message entropy	LEA, described in Section 4.2

3- Symmetric Encryption

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

In [25], ZH.Xin et al, propose two new broadcast authentication protocols based on delayed key disclosure. Their protocols are based on symmetric-key cryptographic primitives and rely on cryptographic puzzles to provide efficient broadcast authentication in a wide range of application scenarios, including those with resource-constrained wireless devices such as sensor nodes. The first protocol (BAP-1) achieves instantaneous message-origin authentication upon message reception. Their second protocol (BAP-2) achieves broadcast authentication using a single transmission per authenticated message.

3-1- BAP-1 Protocol

The protocol achieves broadcast authentication through delayed key release based on cryptographic puzzles. Instant message authentication is achieved if the receiver solves the puzzle, and therefore obtains the key, before receiving the message. All messages received by B are marked with ' to denote that they might have been modified in transit by an attacker. BAP-1 is designed to achieve instantaneous message verification upon message receipt.

3-2- BAP-2 Protocol

The protocol achieves broadcast authentication through delayed key release based on cryptographic puzzles. Message authentication is achieved if the receiver receives the puzzle before the attacker has solved the puzzle. All messages received by *B* are marked with ' to denote that they might have been modified in transit by the adversary.BAP-2 is based on an approach similar to BAP-1 in that late key disclosure is achieved using cryptographic puzzles. The main difference is that in BAP-2, not only the key, but also the message and its MAC are encapsulated within a puzzle. This collapses three messages into one and also reduces the time that the attacker has to solve the puzzle in order to break the scheme.

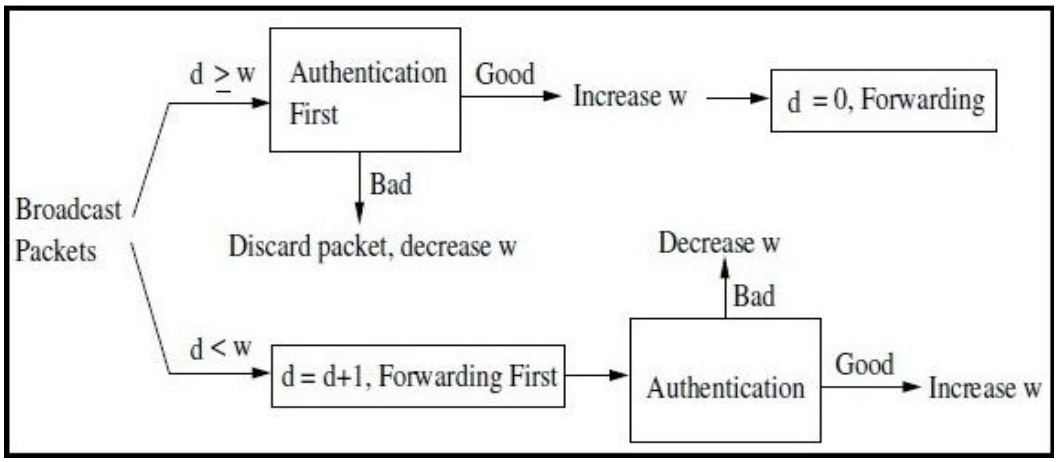

Figure 3: Illustration of Dynamic Window Scheme

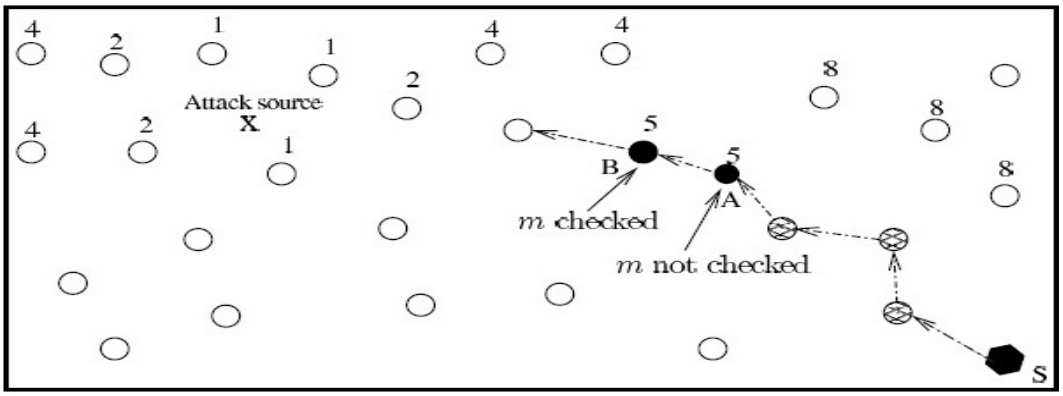

Figure 4: Example of Dynamic Window Scheme

In [13] S.Chang, at al, proposes a computationally lightweight one-time signature scheme that allows sensor nodes to authenticate broadcast messages from a base station in a wireless sensor network. To attain the asymmetric property necessary for broadcast authentication, they utilize symmetric cryptographic primitives. Moreover, they mitigate the general drawbacks of one-time signature schemes: the use of an extremely large key size and the limitation to authenticate only a few messages. The proposed scheme efficiently reduces the storage requirement and includes a re-keying mechanism to sign additional messages.

3-3- Message Authentication Code (MAC)

A MAC is a symmetric cryptographic mechanism that takes as input a k-bit secret key and a message, and outputs an l-bit authentication tag. To exchange authentic messages, a sender and receiver must share the same secret key. Using the secret key, the sender computes the message's authentication tag (or MAC) and appends it to the message. To verify the authenticity of a message, the receiver computes the message's MAC with the secret key and compares it to the original MAC appended with the message. For any message, a secure MAC function prevents an attacker without prior knowledge of the secret key from computing the correct MAC. A MAC achieves authenticity for point-to-point communications because a receiver knows that a message with the correct MAC must have been generated either by itself or by the sender. A Merkle hash tree can reduce the authentication overhead needed for a large group of data items. For example, a sender signs the root of the tree instead of individual data items. The receiver can then verify the authenticity of every data item by reconstructing the tree and comparing the computed hash value of the tree, which they call *hash tree*, with the authenticated root value.

To reconstruct the tree, the receiver needs all of the data items. An alternative is for the receiver to verify a data item individually by computing the hash tree using the data item and its authentication path. Illustrated in Figure 2-3, the *authentication path* of the leaf is the value of all nodes that are siblings of nodes on the path between the leaf and the root.

To support an amount of dynamic users with low communication and computation overhead, S.Yoon , at al, propose a hybrid multi-user broadcast authentication scheme by adopting public key concept into µTESLA.

A typical place to perform broadcast authentication is at the ends of communication, which means that forwarders do not check the integrity of packets. This broadcast authentication scheme residing at application layer can be considered as a scheme using "forward-first" policy: a node rebroadcasts each packet if needed and then delivers authentic ones to application after signature validation. Pure "forward-first" scheme misses the containment capability. A false packet is broadcast everywhere before its authenticity is verified. In order to contain false packets, an intuitive way is to apply hop by hop authentication scheme based on "authenticate-first" policy at routing layer: a node only rebroadcasts authentic messages after validation. In this way, false packets are filtered out at the first hop and devices outside the transmission range of attackers are immune. However, this hop-by-hop authentication scheme imposes remarkable penalty on end to end delay of legitimate traffic due to authentication delay at each intermediate hop. The accumulated delay postpones packet delivery to nodes far away from the sources and the maximal delay is proportional to network diameter in hops.

In [21], Y.Huang, at al, present a novel broadcast authentication scheme, called DREAM, an acronym for DoS-Resistant Efficient Authentication Mechanism. It effectively limits false data injection via frequently using "authenticate-first" policy based on public-key authentication. It also reduces the end to end delay by allowing a small percentage of unverified packets forwarded probabilistically via "forward-first" policy so that remote nodes obtain the broadcast messages quickly. Compared with most pertinent work considering containment of false broadcast injection [13, 23, 26], DREAM offers the following two advantages: (1) the remote nodes, who receive the unverified packets, are randomly determined for each packet. Hence, DREAM avoids a single point of failure and achieves load balancing. (2) In order to reduce end-to-end delay, not everyone in the neighborhood of a broadcast source has to forward unverified packets. Allowing only a small number of packets to reach remote regions is sufficient to reduce delay, while it effectively restricts contagious areas of false packets.

Lamport's Scheme

Hash chains were first proposed by Lamport [27]. They involve applying a hash function h (×) N times to a seed (s) to form a hash chain of length N:

$$H^1(s), h^2(s), h^{N(s),h} N^{(s)}$$

The user calculates the *i*-th key according to this relation:

$K_i(s) = h^{N-i}(s)$

The host authenticates the user by checking that the following equality holds:

$h(k_t(s)) = h^{N-i+1}(s)$

Where the value $h^{N-i+1}(s)$ is already saved in the host system's file from the previous *i*-th authentication. After any successful authentication, the system password file is updated with the new key. This scheme has a limitation on the number of authentications, so that after reaching *N* authentications, a process restart is required. In addition, it is vulnerable to an opponent who sends small challenge values to users that respond with the chain initial values [27]. This attack can be referred to as a small challenge attack. Also, the users are charged with computational processes through the initialization phase, which makes the system unsuitable for WSNs.

4-1 Chinese Remainder Theorem (CRT)

If the integers n_1, n2… nk are pair-wise relatively prime, then the system of simultaneous congruence:

$X = r_1 \bmod n_1$

$X = r_2 \bmod n_2$

.

.

.

$X = r_k \bmod n_k$

Has a unique solution: $x = \sum_{i=1}^{k} r_i N_i^{-1} N_i \; mod \; N$ where:

$$N = \prod_{i=1}^{k} n_i$$

$N_i = \frac{N}{n_i}$

$N_i^{-1} N_i \equiv 1 \; mod \; n_i$

The basic idea of this scheme is to expand Lamport's scheme [27] with some modifications that produce the desirable infiniteness and forwardness, avoiding the use of public key cryptography. The shortcoming of those two parameters, infiniteness and forwardness, causes the insufficiency shown with respect to the previous work.

4- µTESLA

Broadcast authentication in WSNs was first addressed by µTESLA [15]. In µTESLA, users of WSNs are assumed to be one or a few fixed sinks, which are always assumed to be trustworthy. The scheme adopts a one-way hash function h () and uses the hash preimages as keys in a message authentication code (MAC) algorithm. Initially, sensor nodes are preloaded with K0 = $h^n(x)$, where x is the secret held by the sink. Then, K1 = hn¡1(x) is used to generate MACs for all the broadcast messages sent within time interval I1. During time interval I2, the sink broadcasts K1, and sensor nodes verify h (K1) = K0. The authenticity of messages received during time interval I1 are then verified using K1. This delayed disclosure technique is used for the entire hash chain and thus demands loosely synchronized clocks between the Sink and sensor nodes. µTESLA is later enhanced in [18, 19] to overcome the length limit of the hash chain.

Most recently, µTESLA is also extended in [4, 18] to support multiuser scenario but the scheme assumes that each sensor node only interacts with a very limited number of users.

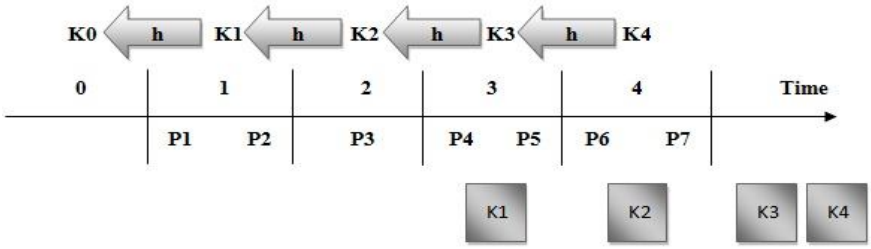

Figure 5: The µTESLA One-Way Key Chain

It is generally held that µTESLA-like schemes have the following shortcomings, even in the single-user scenario:

1) All the receivers have to buffer all the messages received within one time interval.
2) They are subject to Wormhole attacks [20], where messages could be forged due to the propagation delay of the disclosed keys.

However, here, we point out a much more serious vulnerability of µTESLA-like schemes when they are applied in multihop WSNs. Since the sensor nodes buffer all the messages received within one time interval, an adversary can hence arbitrarily flood the whole network. All the adversary has to do is to claim that the flooding messages belong to the current time interval, which should be buffered for authentication until the next time interval. Since wireless transmission is very expensive in WSNs and WSNs are extremely energy constrained, the ability to arbitrarily flood the network could cause devastating Denial of Service (DoS) attacks. Moreover, these types of energy-depletion DoS attacks become more devastating in a multiuser scenario as the adversary can now have more targets and, hence, more chances to generate bogus messages without being detected. Obviously, all these attacks are due to the delayed authentication of the broadcast messages. In [20], the TIK protocol is proposed to achieve immediate key Disclosure and, hence, immediate message authentication based on precise time synchronization between the sink and receiving nodes.

In [17], J.Drissi at al , first overview the design of L-TESLA (Localized TESLA). Then, they give two core algorithms in L-TESLA. Finally, they use an example to demonstrate LTESLA.

Assuming normal nodes and trusted nodes are already deployed in a target area. Since the number of trusted nodes is small, each node can remember the IDs of all trusted nodes. Many key distribution approaches [17, 21] have been proposed for sensor nodes to establish pair wise keys. However, in this paper, they only ask each node to set up secret keys with the trusted nodes for exchanging a few LTESLA messages. To further secure the network, they use the secure key revocation technique [22] to prevent a compromised trusted node from disclosing the secret keys. Because a trusted node can have more computation, storage and power resources, they let each trusted node generate and maintain two key chains: a global chain for TESLA and a local chain for L-TESLA.

L-TESLA works in two phases. In the first phase, each trusted node broadcasts a request (BREQ) which is secured by TESLA with its global key chain. The BREQ helps all other nodes to first their nearby trusted nodes for the source of the BREQ. Thereby, the area is divided into several local areas. In each local area, a trusted node can use its L-TESLA to rebroadcast messages while reducing the verification delay in the second phase. After all trusted nodes broadcast BREQ, a secure broadcast mesh is established in the area so that: (a) each trusted node has a verification delay and maintains a local key chain for its local TESLA, and (b) all nodes know from which upstream trusted node they should receive and verify a broadcast message according to the source of the message. In another words, the first phase uses the traditional TESLA to bootstrap local TESLA in the second phase.

In the second phase, when a node needs to broadcast a message (BPKT), it first sends the message to its closest trusted node. Then, the trusted node broadcasts the message by using its local TESLA. Upon receiving the broadcast message, a normal node will rebroadcast the message as long as the message is secure, first time received, and from its selected upstream trusted node. Nevertheless, a trusted node will transform the message with its own local TESLA information. Note that all nodes verify the BPKT based on the local TESLA of their selected upstream trusted node.

In [5], K.Ren, at al, propose four different public-key-based approaches and provide indepth analysis of their advantages and disadvantages. In all the four approaches, the users are always authenticated through their public keys. They first propose a straightforward certificate-based approach and point out its high energy inefficiency with respect to both communication and computation costs. They then propose a direct storage based scheme, which has high efficiency but suffers from the scalability problem. A Bloom filter based scheme is further proposed to improve the memory efficiency over the direct storage based scheme. Further techniques are also developed to increase the security strength of the proposed scheme. Lastly, they propose a hybrid scheme to support a larger number of network users by employing the Merkle hash tree technique. they give an in-depth quantitative analysis of the proposed schemes and demonstrate their effectiveness and efficiency in WSNs in terms of energy consumption.

3-Dos-Resistant

Currently, one of the most destructive kinds of attacks is Denial of Service (DoS), primarily its distributed form DDoS (Distributed DoS). For the attacker, it is quite easy to overload selected server or whole network. Vulnerability to DoS attacks is much more striking in broadcast communication when each packet should be delivered to all nodes in the network. If the attacker is able to generate a sufficient number of packets, the whole network can be overloaded. It is possible to avoid such incident by verifying the origin of each packet in the network before its processing in the node. However, in the network whose nodes have limited computing power and memory (typical for sensor networks), each authentication process using traditional public key cryptographic techniques is quite burdensome. A big number of these calculations lead to growth of time that the packets spent in the network and communication among nodes becomes almost impossible. In the case of broadcast communication, this issue can be efficiently solved by DREAM (DoS-Resistant Efficient Authentication Mechanism) [17] protocol.

3-1 DREAM Protocol

DDoS is so powerful since it uses multiple systems as resources of the attack and therefore, it is much stronger than a single sourced attack. DREAM mitigates the DDoS impact by involving an analogous approach which the DDoS uses itself. The only difference is that more stations are involved in the process of verification. The DREAM protocol can operate in two modes: normal and secure. Every incoming message is authenticated by the network node before being sent to the outgoing interface in the secure mode. In the normal mode, some of the messages are sent directly to the outgoing interface without being authenticated. This approach mitigates the potential single point of failure in the whole network since there is not a single node where authentication occurs. The verification process is distributed among the neighboring nodes. The protocol functionality is influenced by the following parameters [5]:

- *NBR* – number of neighbors.
- *HT* – number of nodes that message passed without authentication. For such each node, the parameter is incremented by one. When the packet is authenticated *HT* is set to zero.

- *K* – Maximum number of nodes, that can message pass without authentication.
- *b* – Expected number of neighbors in unity distance from the source.
- *c* – Expected number of neighbors in unity distance from the last node that forwards the message.
- The amount of messages to be sent or verified before sending out the interface is defined by the following decision rules (formulas) [5]:
- Rand $<\frac{b}{NBR}$, (1)
- Rand $<\frac{2c}{NBR}$, (2)
- Where *Rand* is a random number generated independently by every node for every message in the range of 0 and 1 with the continuous uniform distribution [17]. The first formula is used when the message comes directly from a neighbor, a neighbor has been verified, or the parameter $HT = 0$. The second formula is used if the message did not come from a neighbor, or a neighbor has not been verified, or the parameter $HT > 0$.
- In [23], D.Liu et al, propose an extension to µTESLA to address the above limitation. The basic idea is to predetermine and broadcast the initial parameters required by µTESLA instead of unicast-based message transmission. In the simplest form, their extension distributes the µTESLA parameters during the initialization of the sensor nodes (e.g., along with the master key shared between each sensor and the base station). To provide more flexibility, especially to prolong the life time of TESLA without requiring a very long key chain, they introduce a multi-level key chain scheme, in which the higher-level key chains are used to authenticate the commitments of lower-level ones. To further improve the survivability of the scheme against message loss and Denial of Service (DOS) attacks, they use redundant message transmission and random selection strategies to deal with the messages that distribute key chain commitments. The resulting scheme removes the requirement of unicast-based initial communication between base station and sensor nodes while keeping the nice properties of µTESLA (e.g., tolerance of message loss, resistance to replay attacks). Their implementation and experiments further demonstrate that their scheme can tolerate high channel loss rate and is resistant to certain known DOS attacks to a certain degree.
- A desirable property of conducting authentication before forwarding is no faked broadcast messages will be propagated, which is desirable for tolerating DoS attacks. An ideal solution is to conduct authentication-first for faked messages, and forwarding-first for authentic ones.

However, this is hard to achieve, because sensor nodes have no idea on whether they are first hop victims of the attackers or not. In [24] R.Wang et al, propose a dynamic window scheme that is the combination of the authentication-first and the forwarding-first scheme, which can achieve a good trade-off between the broadcast delay for authentic messages and energy savings for faked messages.

- The basic idea of their scheme is that, sensor nodes gradually shift to authentication-first scheme if they start receiving many faked messages, but will remain in forwarding-first mode if the majority of the messages they receive are authentic. The decision is based on the validity of the incoming broadcast messages they receive. Every broadcast message keeps record of the number of hops it has passed since its last authentication, and sensor nodes maintain an authentication window size, which will be updated dynamically. Based on both the window size on sensor nodes and the number of hops the incoming message passes after its last authentication, the nodes decide which mode to use: if window size is the larger, they use forwarding-first mode; otherwise, they use authentication first mode. In their scheme, they use Additive Increase Multiplicative Decrease (AIMD) techniques to dynamically manage the window size on sensor nodes: if the message they receive is authentic, the window size increases; otherwise, window size decreases.

3.2-Attacking Model

In [24], R.Wang et al, assume that the goal of the attackers is to exhaust the energy of the sensor nodes, and to increase the response time of the sensor nodes to the authentic broadcast messages. The primary attacking method of the adversaries is to broadcast large number of faked messages. In order to fool honest nodes, attackers may forward authentic messages from time to time. To implement the attack, adversaries can compromise honest nodes, or deploy malicious sensors of their own. There are other types of DoS attacks such as jamming or black hole attack, but they do not consider them in that paper. They assume that the attacks are static: adversaries, as well as sensor nodes and base stations, stay in fixed locations throughout the attack. That is, the topology of the network is fixed. Attackers can choose their locations, or take multiple identities, but they cannot move during the attack.

Their goal is to defend sensor networks against DoS attacks, especially the type of attacks that aim at exhausting the energy of sensor nodes. Due to the wireless nature of sensor networks, it is impossible to design a scheme that is totally immune to DoS attacks, so their goal is to reduce the damage of the attacks on the entire network. In other words, they want to contain the damage of DoS attacks to a small portion of the sensor nodes.

3-3 Dynamic window scheme

Dynamic window scheme is an efficient yet effective protocol that can contain the damage of DoS attacks to a small portion of the sensor nodes. AIMD itself is not a new idea; it has been used in congestion control in sensor networks as well as in general networks. However, designing a DoS resistant scheme for broadcast authentication in sensor networks is not a trivial extension of previous works: sensor nodes have no idea on who is malicious and who is not. What is more, sensor nodes are extremely resource-constrained, and they should not be carried away by the overwhelming attacks from the adversaries. The design of this DoS resistant scheme is an important contribution of this scheme.

Table2: Summarizes the Authentication Techniques

Scheme	Authentication	Scalability	Communication cost	Communication speed
ESUAS	Unilateral	No	High	Less
IDUAS	Unilateral	Yes	High	Less
RDUAS	Mutual	No	High	Less
LUAS	Mutual	Yes	High	Less
ATTUA	Unilateral	Yes	Less	Less

Table3: Schemes properties

Scheme	Properties
L-TESLA	• management advantage in a large sensor network for TESLA • reducing the verification delay • application delay of a node
DREAM	DoS-Resistant
dynamic window	• is the combination of the authentication-first and the forwardi • can achieve a good trade-off between the broadcast delay for a
BAP-1	• the send key to a puzzle before the message • is designed to achieve instantaneous message verification upon • The protocol achieves broadcast authentication through delaye • only key is encapsulated within a puzzle
BAP-2	• reduces the communication overhead in terms of the number c • the key and the message and its MAC is encapsulated within a
MAC	• symmetric cryptographic • Cheep
symmetric cryptogr	• much more efficient than asymmetric primitives • symmetric cryptographic
H-MBA	• support an amount of dynamic users with low communication • Broadcast efficiency • Security

Table4: Point to Point and Broadcast Properties

point to point and Broadcast properties	
point to point properties	**Broadcast properties**
can be achieved through purely symmetric	authenticated broadcast requires an asymmetric mechanism
Authentication of point to point messages in sensor networks is much easier than broadcast authentication	Authentication of broadcast messages in sensor networks is much harder than point-to-point authentication
an entity authenticates itself to a single entity	an entity authenticates itself to all entities in the network

Table5: Schemes Properties

Scheme	security	Mac	Symmetric	Point to Point	Broadcast	DoS-Resistant	support a large number users
µTESLA		√			√		no
L-TESLA					√		no
Multi User					√		no
MAC	√	√	symmetric	√			
DREAM	√				√	√	
GBA	√		Asymmetric		√	√	
BAP-1		√	symmetric		√		
BAP-2		√	symmetric		√		
dynamic wind	√				√	√	
H-MBA	√		symmetric		√		yes

References

Akyildiz, I.F., et al., A survey on sensor networks. Communications magazine, IEEE, 2002. **40**(8): p. 102-114.

Ren, K., et al., On broadcast authentication in wireless sensor networks. Wireless Communications, IEEE Transactions on, 2007. **6**(11): p. 4136-4144.

Akyildiz, I.F. and I.H. Kasimoglu, Wireless sensor and actor networks: research challenges. Ad hoc networks, 2004. **2**(4): p. 351-367.

Liu, D., et al. Practical broadcast authentication in sensor networks. in Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on. 2005: IEEE.

Ren, K., et al., Multi-user broadcast authentication in wireless sensor networks. Vehicular Technology, IEEE Transactions on, 2009. **58**(8): p. 4554-4564.

Undercoffer, J., et al. Security for sensor networks. in CADIP Research Symposium. 2002: Citeseer.

Yeh, H.-L., et al., A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 2011. **11**(5): p. 4767-4779.

Karlof, C., N. Sastry, and D. Wagner. TinySec: a link layer security architecture for wireless sensor networks. in Proceedings of the 2nd international conference on Embedded networked sensor systems. 2004: ACM.

Menezes, A.J., P.C. Van Oorschot, and S.A. Vanstone, Handbook of applied cryptography. 2010: CRC press.

Perrig, A., et al., SPINS: Security protocols for sensor networks. Wireless networks, 2002. **8**(5): p. 521-534.

Kahn, J.M., R.H. Katz, and K.S. Pister. Next century challenges: mobile networking for "Smart Dust". in Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking. 1999: ACM.

Hill, J., et al. System architecture directions for networked sensors. in ACM SIGOPS operating systems review. 2000: ACM.

Chang, S.-M., et al. An efficient broadcast authentication scheme in wireless sensor networks. in Proceedings of the 2006 ACM Symposium on Information, computer and communications security. 2006: ACM.

Rivest, R.L., A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978. **21**(2): p. 120-126.

Perrig, A., et al., The TESLA broadcast authentication protocol. 2005.

Luk, M., A. Perrig, and B. Whillock. Seven cardinal properties of sensor network broadcast authentication. in Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. 2006: ACM.

Drissi, J. and Q. Gu. Localized broadcast authentication in large sensor networks. in Networking and Services, 2006. ICNS'06. International conference on. 2006: IEEE.

Liu, D. and P. Ning, Multi-Level microTESLA: A Broadcast Authentication System for Distributed Sensor Networks. 2003.

Lu, C., et al. A spatiotemporal query service for mobile users in sensor networks. in Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on. 2005: IEEE.

Yih-Chun, H., A. Perrig, and D. Johnson. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks. in Proc. of the 22nd Annual Joint Conference of IEEE Computer and Communications Societies. Pittsburgh, USA: IEEE Press. 2003.

Huang, Y., et al. DoS-resistant broadcast authentication protocol with low end-to-end delay. in INFOCOM Workshops 2008, IEEE. 2008: IEEE.

Zhou, T. and K. Chakrabarty. Authentication of sensor network flooding based on neighborhood cooperation. in Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE. 2006: IEEE.

Liu, D. and P. Ning. Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks. in NDSS. 2003.

Wang, R., W. Du, and P. Ning. Containing denial-of-service attacks in broadcast authentication in sensor networks. in Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing. 2007: ACM.

ZHAO, X., et al., An efficient broadcast authentication protocol in wireless sensor networks. Chinese Journal of Electronics, 2009. **18**(2).

Vanek, T. and M. Rohlik, Analysis of Broadcast Authentication Mechanism in Selected Network Topologies. Radioengineering, 2011. **20**(1): p. 167.

Schaller, P., S. Čapkun, and D. Basin. BAP: Broadcast authentication using cryptographic puzzles. in Applied Cryptography and Network Security. 2007: Springer.