Secure cluster Communications in modern collaborative and cluster oriented Applications

1Mani. P and 2Shanthakumar. P

1PG Scholar, Department of CSE V. S. B. Engineering College Karur, Tamil Nadu, India.
2Professor V. S. B. Engineering College Karur, Tamil Nadu, India.

Received 28 January 2017; Accepted 22 May 2017; Available online 28 May 2017

Copyright © 2017 by authors and American-Eurasian Network for Scientific Information (AENSI Publication).
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/

ABSTRACT

The wireless network is a connection established between the more than numbers of nodes. The nodes are mobile, laptop, pc, and etc. Thus the node has to be communicating to each other. The communication must be very secure in this method. The source and destination has to be using the asymmetric secret key. Cluster key agreement (CKA) is widely employed for secure cluster communications in modern collaborative and cluster-oriented applications. A popular approach to secure cluster communications is to exploit cluster key agreement (CKA). The key is generated in the Cluster key agreement (CKA) algorithm is widely employed for secure cluster communication in modern collaborative and cluster-oriented application. Design of a dynamic authenticated CKA protocol is based on strongly unforgeable and identity-based batch multi-signatures (IBBMS). Identity-based authenticated cluster key agreement (CKA) protocol is a cluster of users to establish a common encryption key. Although the protocol does not need certificates and is free from key escrow, extra efforts are required to address user dynamicity and provable security. A CKA is identify-based cryptosystems with an emphasis on round-efficient, the sender has to be unrestricted and the member is dynamic. It is allows a more than members dynamically in to the network communication and establish a public cluster encryption key, and each member has a different secret decryption key in an identify-based cryptosystem. Any node of the network is to be encrypting the message using cluster secret key and decrypt the message using unique private key in the destination node.

KEYWORDS: WSN, Diffie-Hellman, CKA Protocol, cluster, IBAACKA, Identity Based Encryption

INTRODUCTION

Advances in wireless communication and Micro Electro Mechanical Systems (MEMS) have enabled the development of low-cost, low-power, multi-functional, tiny sensor nodes which can sense the environment, perform data processing and communicate with each other over short distances. Due to a wide range of potential applications including environment monitoring, object tracking, scientific observing and traffic control and etc., Wireless Sensor Network (WSN) have attracted a plethora of research efforts.

A typical large-scale WSN generally consists of one or more sinks (or base stations) and tens or thousands of sensor nodes that organized themselves into a multi-hop wireless network and deployed either randomly or according to some predefined statistical distribution over a geographical region of interest. A sensor node by itself has severe resource constraints, such as limited memory, battery power, and signal processing, computation and communication capabilities hence it can sense only a small portion of the environment.

However, a cluster head of sensors collaborating with each other can accomplish a much bigger task efficiently. With integration of sensing, computation, and wireless communication, the sensor nodes can sense physical information, process crude information, and report them to the sink or base stations that can make application specific
decisions and link to the outside world via the Internet or satellites. WSN is mainly distinguished from the conventional wireless ad hoc network by their unique and dynamic network topology which owing to the time-varying link condition and node variation, diverse applications focuses on different sensory date requirement in terms of quality of service (QoS) and reliability. Furthermore, sensor nodes’ limitation in power, computational capacities and memory are often deployed in large numbers and high density, for example to sense, process, and disseminate information of physical environments, thus resulting in upstream direction traffic from the sensor nodes to the sink whereas conventional networks are mostly point-to-point or point-to-multipoint data forwarding.

Therefore, one needs to carefully cope with such problems as energy conservation, reliability, and quality of services (QoS) to meet application requirements. Our major in this system focuses on the coverage problem of WSN. Coverage is a fundamental research issue in WSN because it can be considered as the measure of QoS of sensing function for a sensor network. For example, in an application of forest monitoring, one may ask how well the network can observe a given area and what the chances are that a fire starting in a specific location of forest will be detected in a given time frame.

This system presents a thorough survey of the existing coverage schemes for WSN, and it also outlines several open problems. The purpose is to provide a better understanding of coverage technology and to stimulate new research directions in this area. The remainder of the system is organized as follows. We introduce some design criterions in coverage problem for WSN that followed by the related problem in other fields. Next, we classify coverage schemes into three categories: point coverage, area coverage and path coverage, what is more, we make a summary and comparison of existing coverage scheme for WSN.

The coverage problem is centered on a fundamental question how well do the sensors observe the physical space. On some occasions, we need to consider about coverage (Given any integer k, a monitored region R by WSN if and only if each point in R is covered by at least k sensors). For example, in wireless sensor networks, because energy depletion, harsh environmental conditions, and malicious attacks may result in node failures or become inoperative at any time, it is desirable to have higher degrees of coverage. The goal is to have each location in the physical space of interest within the sensing range of at least one sensor. Depended on different objectives and application requirements, there are different factors analyzed in designing coverage schemes. In this way, a fair comparison among existing scheme has to be taken into consideration, since these factors affecting the coverage performance of WSN. Generally, there are many different criterions (factors) can affect the coverage performance of WSN. While it is impractical to cover all the possible factors, in this system we review a wide range of factors that have dominating effect.

Where a sensor can detect an object or phenomena are inside its sensing range deterministically (a sensor can detect an object as long as the object is inside its sensing range) or probably (the detection probability of an object is a function of the distance between the object and the sensor) depended on its sensing model. Generally, the sensors are assumed to have the same range. For example, the sensing area is considered to be isotropic (e.g., a circular area in 2-D). Moreover, there are several mechanisms that are extensible to any convex, no uniform sensing areas or irregular sensing areas.

The rest of the paper is organized as follows. The comprehensive review of the survey of the literature is elaborated along with its pros and cons in section 2. Section 3 explains the proposed architecture obtained based on the literature survey. The simulation results and evaluation are analyzed in the section 4. Section 5 concludes the paper.

**Literature Review:**

In the literature, How to sense and monitor the environment with high quality is an important research subject in the Internet of Things (IOT). [1] Dan Boneh, Alice Silverberg (2016) suggested an application of multi linear forms to cryptography. The cryptography has recently been solved using Weil or Tate pairings on super singular elliptic curves, or more generally on super singular varieties. These applications include one round three-party key exchange, identity-based encryption, and short digital signatures. We show that multi linear generalizations of Weil or Tate pairings would have far-reaching consequences in cryptography. The desired properties for a multi linear form. Such forms would enable secure broadcast encryption with very short broadcasts and private keys, a unique signature scheme, and one-round multi-party key exchange. The main question is how to build the required multi linear maps. We now have the means and the opportunity.

The Key agreement is a cryptographic protocol, [2] where two or more participants, who each have a long-term key, exchange ephemeral messages (alternatively called key tokens) over an open network with each other. Using the long-term keys and key tokens, these participants generate a session secret shared between them. This secret is used to establish a session key and to perform various security functions, for example, key confirmation, entity and data authentication and confidentiality. The open network is controlled by an adversary, who aims to infiltrate the protocol. A secure key agreement protocol guarantees that the adversaries do not succeed. We focus on a special type of key agreement protocols, which are two-party identity based protocols and make use of pairings to compute session secrets. The concept of identity-based cryptography [7], in which a public key is the
identity (an arbitrary string) of a user, and the corresponding private key is created by binding the identity string with a master secret of a trusted authority (called Key Generation Centre), was formulated by Shamir in 1984. In the same paper, Shamir provided the first identity-based key construction based on the RSA problem, and presented an identity-based signature scheme [8][9]. By using varieties of the Shamir key construction, a number of identity-based key agreement schemes were proposed.

[3] Mike Burmester (2004) by a secure and efficient conference key distribution system. The two users want to compute a common key, then a conference key distribution system is used. Designing such systems can be particularly challenging because of the complexity of the interactions between the many users. Many conference key distribution systems have been presented recently. These however are either impractical or only heuristic arguments are used to address their security. Our goal in this paper is to present a practical and proven secure conference key distribution system. Ingemarsson, Tang and Wong proposed a conference key distribution system for which the common key is a symmetric function. This has many attractive features but is insecure because the information exchanged by the users makes it possible for a passive eavesdropper to compute the key. Our system is similar but uses a cyclic function. This prevents the attack by passive eavesdroppers whilst retaining the efficiency of the former scheme.

[14] An Identity Based Encryption (IBE) system is a public key system where the public key can be an arbitrary string such as an email address. A central authority uses a master key to issue private keys to identities that request them. [4] Hierarchical IBE (HIBE) [HL02, GS02] is a generalization of IBE that mirrors an organizational hierarchy. An identity at level k of the hierarchy tree can issue private keys to its descendant identities, but cannot decrypt messages intended for other identities. The first construction for HIBE is due to Gentry and Silverberg [GS02] where security is based on the Bilinear Diffie-Hellman (BDH) assumption in the random oracle model. A subsequent construction due to Boneh and Boyen [BB04a] gives an efficient (selective-ID secure) HIBE based on BDH without random oracles. In both constructions, the length of cipher texts and private keys, as well as the time needed for decryption and encryption, grows linearly in the depth d of the hierarchy. There are currently two principal applications for HIBE. The first, due to Canetti, Halevi, and Katz, is forward secure encryption. Forward secure encryption enables users to periodically update their private keys so that a message encrypted at period n cannot be read using a private key from period n0 > n. To provide for T = 2t time periods, the CHK construction uses a HIBE of depth t where identities are binary vectors of length at most t. At time n, the encryptor encrypts using the identity corresponding to the n-th node of this depth t binary tree. Consequently, using previous HIBE systems [GS02, BB04a], cipher text in this forward secure construction are of size O(t) private keys are of size O(t2) but can be reduced to size O(t) by using updateable public storage [10][11][13]. Key establishment is a process whereby two (or more) entities can establish a shared secret key (session key). There are two different approaches to key establishment between two entities. [5] In one scenario, one entity generates a session key and securely transmits it to the other entity. This is known as enveloping or key transport. More commonly, both entities contribute information from which a joint secret key is derived. This is known as key agreement. All the protocols discussed in this paper are of this form. A key agreement protocol is said to provide implicit key authentication (of B to A) if A is assured that no other entity besides B can possibly ascertain the value of the secret key A key agreement protocol provides key confirmation (of B to A) if A is assured that B possesses the secret key. A protocol that provides mutual key authentication as well as mutual key confirmation is called an authenticated key agreement with key confirmation protocol (or an AKC protocol).

In this system [6] developed three asynchronous algorithms (AMQFH, CMQFH, and nested-CMQFH) for multicast rendezvous in spectrum-heterogeneous DSA networks. To account for PU dynamics, we also designed two channel ordering mechanisms for sequential channel sensing and channel assignment (one for AMQFH and the other for CMQFH and nested-CMQFH). Moreover, we developed a proactive out-of-band sensing based DFH algorithm for online adaptation of the FH sequences used in our rendezvous algorithms. One important advantage of quorum based FH designs is their robustness to synchronization errors. Frequency hopping (FH) provides an effective method for rendezvousing without relying on a predetermined control channel. The change in the cluster head key has to be consistent among all SUs in the multicast cluster head. The prediction accuracy for nested-CMQFH is better than CMQFH, because nested-CMQFH has more deterministically assigned quorum slots than CMQFH (recall that in nested-CMQFH, high quality channels, as obtained from Problem

Proposed Architecture:

System architecture is the conceptual model that defines the structure, behavior, and more views of a system. Fig. 1 an architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.
System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

A sender wants to send a secret message to a cluster head of receivers, the sender has to first join the receivers to form a cluster head and run a CKA protocol [6][12]. A user may also join the cluster head if the number of the protocol participants is smaller than the maximum allowable cluster head size. The KGC (key generation center) is generating the key for all the nodes in the network. This algorithm contains the two or more rounds are used, the entire user has to stay online to finish the protocol before they can receive any encrypted contents. The CKA protocol is generating the symmetric cluster head key that is not secured. Thus problem is overcome in this module. This module is using the asymmetric cluster head key agreement (ACKA). The ACKA is using the KGC (key generation center). The KGC is employed to generate the long-term private keys for the cluster head members. ACKA allows the members to negotiate a common cluster head encryption key while holding different decryption keys. The members to negotiate a common cluster head encryption key while holding different decryption keys. Any user may access the cluster head encryption key and securely encrypt the message and transfer to the cluster head members. This system has to be use the identity-based authenticated asymmetric cluster head key agreement (IBAACKA) protocol without key escrow was proposed, which enables a cluster head of users to establish a common encryption key and their respective encryption keys in one round and thus the protocol does not need certificates and is free from key escrow, extra efforts are required to address user dynamicity and provable security. One round dynamic IBAACKA protocol is proposed and proven secure in our key. It offers secrecy and known key security.

3.1 cluster head key agreement:

The cluster head key agreement with an arbitrary connectivity graph, where each user is only aware of his neighbors and has no information about the existence of other users. Further, he has no information about the network topology. Under this setting, a user does not need to trust a user who is not his neighbor. Thus, if one is initialized using PKI, then he need not trust or remember public-keys of users beyond his neighbors.

The cluster head key agreement methods are performs efficiently when adding or deleting nodes dynamically. It provides authentication of each node for valid member of the cluster head. Cluster head key agreement (CKA) is employed for secure cluster head communications in modern collaborative and cluster head-oriented applications. This protocol requires two or more rounds to establish a secret key. CKA protocols allow a cluster head of members to interact over an open network to establish a common secret key and cluster head members can securely exchange message using this shared key.

The sender has to be sending the secret message to a cluster head of receivers, a cluster head of users in
different time zones would like to discuss some sensitive topics via an untrusted third party. Each member of one unit has to first run the CKA protocol with the members of the other unit in a different battlefield. This is almost prohibitive given the poor communication environment in battle scenarios and it is difficult for users in different time zones.

3.2 Key pre distribution system:
Key pre-distribution system (KPS) (a.k.a. non-interactive conference distribution system) can be regarded as a non-interactive cluster head key agreement. In this case, the shared key of a given cluster head is fixed after the setup. If a cluster head is updated, then the cluster head key changes to the shared key of the new cluster head. The drawback of KPS is that the user key size is combinatorial large in the total number of users (if the system is unconditionally secure). Another drawback is that the cluster head key of a given cluster head cannot be changed even if it is leaked unexpectedly (e.g., cryptanalysis of cipher texts bearing this key). The key size problem may be overcome if a computationally secure system is used, while the key leakage problem is not easy. Further, computationally secure KPS is only known for the two-party case and the three-party case. KPS with a cluster head size greater than 3 is still open.

3.3 Diffie Hellman protocol:
The computationally secure cluster head key agreement in a passive model. This started from the Diffie-Hellman protocol. In the following, we use the tuple $(a; b; c)$ to represent a protocol that has $a$ rounds, $b$ elements of messages per user (the unit is a field element in $Z_p$ for a large prime $p$) and computation cost $c$. designed a cluster head key agreement for $n$ users in a ring with an efficiency tuple Their protocol assumes a complete connectivity graph.

Steiner et al. proposed three protocols, where the most efficient one has an efficiency tuple we now survey the computationally secure cluster head key agreement in an active model. The proposed protocols in the random oracle model, where the interesting construction has an efficiency tuple . formalized a formal model for a cluster head key agreement in the active model and made the protocol in actively secure using a signature based authentication.

3.4 Network model:

Fig. 2: CKA protocols structure

Fig.2 The system also proposes security framework and architecture to integrate existing technologies with WSNs in order to provide secure and private communications to its users. Advantages the protocol must establish a key between all sensor nodes that must exchange data securely. Node addition, deletion should be supported. It should work in undefined deployment environment. Unauthorized nodes should not be allowed to establish communication with network nodes. Key chain authentication as well as key revocation and key refreshing.

Fig.3 illustrates scalability able to perform cluster head communications. Implemented Modules Cluster head Key Agreement Protocols HKAP Protocol CKA WSNs Key Generation Center (KGC) Secure effective key management. Cluster head Key Agreement Protocol Cluster head-based CKA protocols, only and provide authentication.
Authentication ensures those only valid cluster head members participate in the key setup phase and therefore provides a way for protection against man-in-the-middle attacks during the key agreement phase. In works and the authors proposed way for turning their protocol into an authenticated one, but they do not specifically analyze the additional communication and computation cost introduced in the protocol by authenticating every message.

*Simulation Results And Evaluation:*

In this section, Simulation results verify that the proposed solution outperforms others in terms of relocation time, total energy consumption, and minimum remaining energy. We use simulation to evaluate the performance of our techniques in terms of throughput, end to end delay, data route success ratio.

In the proposed work by applying clustering method, so the sink can collect information from cluster head and each node. So as a result the delay and packet drop can be reduced.
Fig. 5: graph showing throughput when increasing number of nodes

Fig. 6: graph showing end to end delay when number of node increases

4.1 Comparison of protocols:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Comp cost</th>
<th>Average size</th>
<th>Round</th>
<th>d(g*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joux’s</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>one-round</td>
<td>6</td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Pop</td>
<td>9</td>
<td>4</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Snap</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>smtp</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Diffie Hellman</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

Conclusion:
The proposed method produced better results compared to the existing method. The dynamic CKA (cluster head key agreement) protocols, in which an attacker is allowed to learn the master secret of the KGC (key generation center). A one-round dynamic IBAACKA (identity-based authenticated asymmetric cluster head key agreement) protocol is proposed and proven secure in our model under the k-BDHE assumption. It offers secrecy and known-key security, and it does not suffer from the key escrow problem. Therefore, not even the KGC can decrypt the cipher text sent to a cluster head.

REFERENCES