IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

nCORETech 2017

LBS College of Engineering, Kasaragod

Vol. 6, Special Issue 3, March 2017

Key Establishment using GDH in Wireless Sensor Networks

Ms. Seetha Das V

PG Scholar, LBS College of Engineering, Kasargod, Kerala, India

Abstract: Wireless sensor networks consist of autonomous sensor nodes attached to one or more base stations. Security is critical for many sensor network applications. Traditional key management techniques, such as public key cryptography or key distribution center (e.g., Kerberos), are often not effective for wireless sensor networks for the serious limitations in terms of computational power, energy supply, network bandwidth and defection of center authority. In order to balance the security and efficiency using group key agreement protocol and also support dynamic operations like join, leave, merge, etc. by using ECC based Diffie Hellman key exchange. This protocol employs ternary tree like structure instead of binary tree in the process of group key generation.

Keywords: ECC, group key agreement, ternary tree, ECC based Diffie-Hellman.

I. INTRODUCTION

Wireless sensor networks have applications in many important areas, such as the military, homeland security, health care, the environment, agriculture, and manufacturing. One can envision in the future the deployment of large scale sensor networks where hundreds and thousands of small sensor nodes form self-organizing wireless networks. Providing security in sensor networks is not an easy task. Compared to conventional desktop computers, severe constraints exist since sensor nodes have limited processing capability, storage, and energy, and wireless links have limited bandwidth. Despite the aforementioned challenges, security is important and even critical for many applications of sensor networks, such as military and homeland security applications.

Since the key establishment is the initial step for secure communication, topics on key establishment, agreement and management has been studied for a long time. However, most of traditional key management schemes cannot be applied to the WSN for the communication and computational limitations. Currently, three main problems of WSN security are becoming hot. The first one is that how to enforce efficient security techniques for the resources-limited WSN. The second one is that how to possess the anonymity when the message are passed on multi-hop media. And the third one is that how to establish secure group communication inside the WSN

The general aim of secure group communication is to construct a common secrete key among the group members like sensors for confidential communication. Although several tree based group key establishment technique like CCEGK , EGK , TGDH, STR , etc. are available in literature, all of which employ a binary tree for computing group key and uses two parties Diffie Hellman key exchange as the basic operation. However there is a ternary tree protocol and uses GDH.2 as the basic operation for the group of restricted size 3k where k is any integer. In order to improve the efficiency of the cryptographic technique the ECC based cryptosystem can play an important role since it offers similar level of security which can be achieve with shorter keys size than existing methods which are based on difficulties of solving discrete logarithms over integers or integer factorization. The use of elliptic curve in public key cryptography was independently proposed by Koblitz and Miller in 1985 and since then, an enormous amount of work has been done on elliptic curve cryptography. This paper proposes ECC based contributory key computation for secure group communication in dynamic environment. The proposed technique organizes the key generation process in ternary tree like structure in which every node can have at most three children as sensor node as in, but there is no restriction of the no of group members (not necessary 3k as in. Ternary tree, since the proposed technique uses ECC approach which has low computation cost and smaller key size, the overheads are reduces and the performance of the protocol improves significantly.

II.EXISTING SYSTEM

A tree based group key agreement protocol called TGDH. TGDH computes a group key derived from contribution of all group members using a binary tree. Compared to GDH, TGDH just needs constant rounds to agree up on a common group key and has some computational advantages. Now a days a number of tree based group key agreement protocols have been proposed based on TGDH.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
nCORETech 2017
LBS College of Engineering, Kasaragod
Vol. 6, Special Issue 3, March 2017

III. RELATED WORK

Several approaches have been proposed for group key generation in current literature. These approaches can be classified into three categories: Centralized, Decentralized and distributed approaches
In Centralized approaches an entity usually called key server, is responsible for generation and distribution of group key to all members of the group a trusted third party (TTP) can make this possible. However the main problem with this approach is the TTP must be constantly available and in every possible subset of group there must be a TTP available in order to support continued operation in the event of network partitions.
In decentralized approaches the whole group is split into small subgroups. Each subgroup is managed by Subgroup Controller (SC) which minimizes the problem of concentrating the work on a single point. The failure of one SC will not escort to the failure of the whole group. But also in most of the decentralized technique, the SC may become a bottleneck because the SC must decrypt the group messages and then re encrypt it using the sub key.
In distributed approaches, the group key is generated in a contributory fashion, where all members contribute their own share in computing the group key. Steineret alextended the Diffie Hellman protocol, which is the first pioneering two party key agreement protocols, to multi-party scenario. The Group Diffie Hellman key agreement protocol (GDH) require N rounds to agree up on a common session key for a group of N members. In particular, the number of rounds may be crucial in a large number of group member's environment, because members can't communicate until the other members finish the foregoing round protocol.

IV.PRELIMINARIES

The paper based on ternary tree approach with ECC based GDH as its basic operation, the ECC and ECDH techniques are described in this section.

A. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller(IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements i.e., an elliptic curve system could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key.
In ECC non-singular type of Elliptic curves over the real number are used. The elliptic curve over real numbers takes the general form as:

$y^2 = x^3+ax+b$

In cryptography, variables and coefficients of elliptic curve equation are restricted to elements in a finite field. Thus for above equation x, y are co-ordinates of GF(p), and are integer modulo , satisfying $4a^3+27b^2 \neq 0 \bmod(p)$
(for nonsingular elliptic curve).Where is a modular prime integer which make the EC of finite field. An elliptic curve E over GF(p) consist of points (x,y) defined by above two equations, along with an additional point called O (point at infinity or zero point) in EC. The 'O' point plays the role of identity element for EC group.
Usually an elliptic curve is defined over two types of finite fields: the prime field F_p containing p elements (prime curve) and the characteristic 2 finite field containing 2^m elements (binary curve).This paper focuses on the prime finite field as the prime curve are best suit for software applications .

Elliptic Curve Arithmetic

Cryptographic schemes based on ECC rely on scalar multiplication of elliptic curve points. Given an integer k and a point P€E(F_p), scalar multiplication is the process of adding P to itself k times. The result of this scalar multiplication is denoted k× P or kP.
Points addition and point doubling form the basis to calculate EC scalar multiplication efficiently using the addition rule together with the double-and-add algorithm or one of its variants. The detail description of ECC (including its point addition rule) can be found in various papers including.
The security of ECC based protocols are based on intractability of Elliptic Curve Discrete Logarithm Problem (ECDLP). ECDLP state that: Given P, Q €E , find an integer k€ Z*p such that Q = kP. It is relatively easy to calculate Q given k and P, but it is relatively hard to determine k given Q and P.

B. Three Parties Elliptic Curve Diffie- Hellman Protocol

Three parties Elliptic Curve Diffie-Hellman Protocol based on GDH.2 discussed in implemented with elliptic curve for the group of three sensor nodes (A, B &C) as follows:
1) A, B and C chooses their own private keys a1, a2, a3 €Z* respectively and keep it secret.
2) A calculate X = a1 P and send to B.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
nCORETech 2017
LBS College of Engineering, Kasaragod
Vol. 6, Special Issue 3, March 2017

3) B calculates Y1 = a2 P; Y2 = a2X and construct the set {X (as received from A), Y1, Y2 } which is then transmitted to C.
4) C calculates K = a3Y2; Z1 = a3Y1 and Z2 = a3X. It keeps secret 'K' as the contributory group key and broad cast remaining {Z1,Z2} to the sensor A and B.
5) On receiving from C each member can calculates same group key as
A: K = a1Z1. ; and
B: K = a2Z2.
On completing all three members have a common point in the elliptic curve i.e. K = a3Y2 = a1Z1 = a2Z2 = a1a2a3P. If this secret key is to be used as a session key, a single integer must be derived. There are two categories of derivation: reversible and irreversible [26]. If the session key is also required to be decoded as a point in elliptic curve, it is reversible. Otherwise, it is irreversible. The reversible derivation will result in a session key which doubles the length of the private key. In the irreversible derivation, we can simply use the X-coordinate or simple hash function of the X-coordinate as the session key.

V. METHOD

The proposed protocol chooses a k-bit prime p and determine following public parameters:{Fp, E/Fp, G, P}. where E/Fp: Elliptic curve over Fp.
G: Cyclic additive points group formed by points on
E/Fp.
P: Generator of G.
The protocol describes operation to generate common
Session key among n members (it is not important whether n is equal to 3k or not) called Initialization operation along with others group operations like Join, Leave, Merge, etc. for dynamic group.
1.Initialization
Let us suppose all sensors identified by M1,M2,..., Mn are arranged as the leaf nodes of a ternary tree. Now each member Mi randomly chooses a secrete ai€ Zp* that is assigned by the base station initally (for i =1to n) and keep it safe. The sequence of operations in each round are follows.
1) In first round all sensors are arranged in $\lfloor n/3 \rfloor$subgroups having set of three members in each. (If n is not the multiple of 3 then remaining one or two members supposed to forward in next round and they does nothing in current round. The same condition is in every round) Member in every set form their own common EC points by using ECC based Three Parties Diffie Hellman key exchange .
At the end of first round every subgroup has its own secret key (a point in EC group) in the form of (axi.ayi.azi.P) for i=1... $\lfloor n/3 \rfloor$Where axi, ayi &azi are private keys of first ,second and third member of i'th subgroup.
One member from every subgroup comes forward as the group controller (GC) for the next round. In this way we treat every subgroup as a new node controlled by their GC.
2) In second round There are total $\lfloor n/3 \rfloor$nodes (along with the remaining node coming from previous round) form the subgroups having set of three participants of each and calculates their secrete subgroup key as in previous. This time GCs uses x- co-ordinate of their own subgroup keys as the private key. GC1 calculate (x1.P) and unicast to GC2. GC2 calculates (x2.P) and (x2. x1.P) and broadcast {(x1.P) ,(x2.P),(x2.x1.P)} to the all members of third subgroup. The members of third subgroup now can calculate common key as (x3. x2.x1.P) and keep it secret .GC3 additionally calculates {(x3.x1.P), (x3.x2.P)} and broadcast to the all members of its sibling groups. All sibling subgroup members calculates common key by multiplying their own private value.
Note that GC1, GC2 and GC3 are group controllers and x1, x2 and x3 are their x co-ordinates of common points of first, second and third subgroups respectively.
3) Repeats the above process in subsequent rounds .In every round no. of sensor nodes becomes (1/3) of the previous round. After$\lceil log_3 n \rceil$ rounds we have a single group which includes all the members, each sharing the group secret key.
4) If in last round the no of participants remains only two then instead of three parties it employs two parties ECC based Diffie Hellman for calculating final group key.

An example to initialize 12 (12 ≠ 3k) members by above protocols is illustrated in Figure 1. Members of the group are represented by leaf sensors (or nodes) M1,..,M12. In First round four groups are formed with their own group key shown as the parent nodes G1…G4 of corresponding members. Only one group G5 is possible in second round with participants G1, G2 and G3 they form a common key which is shared by all the members of G1, G2 and G3. Group G4 doing nothing in this round forwarded to the next round. In third round remain only two participants G4 and G5 .They employ two parties ECC based Diffie Hellman as suggested in our protocol to compute final group key which is shared by all the members M1,..,M12.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
nCORETech 2017
LBS College of Engineering, Kasaragod
Vol. 6, Special Issue 3, March 2017

2 Join Operations:
Efficient Join and Leave algorithms are very important to the dynamic group key agreement protocols, since any sensor node can leave and join the group at any time. The proposed protocol handles the join operation in two ways: single join when only one new member wants to join the group and mass join when multiple new members want to join the existing group. When a join request is come to the GC it wait till the predefined thresholds (a small time slot) if more join requests are come within the threshold then these requests are handled by mass join operation. On the other hand in case of single request it is handled by single join operation.

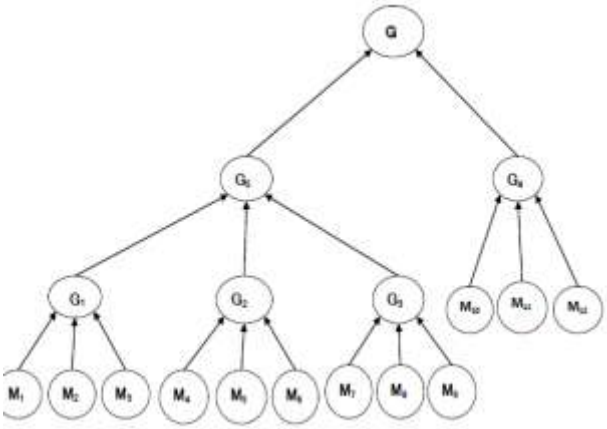

Figure 1: Initialization of 12 Members

4.2.1 Single join
For single join the GC of initial group do the two parties Diffie Hellman Key exchange with the new member. So there are only two messages are required for single join. Initially joining sensor choose a secrete value anew €Zp* and calculate blind key as (anew.P) and broadcast to the members of current group. All members of current group (including GC) can calculates new group key Knew = (x.anew.P) and keep it secret .Now GC of current group send (x.P) to the new member and then the new member can calculates Knew = (anew.x.P). Note that 'x' is the group secret of existing group. The total no. of point multiplications require in single join is: (n+2).

4.2.2 Mass Join
Suppose there are 'm' new sensors are want to join the current group with 'N' members having common group key K then:
a) First initialize 'm' sensors to form their own independent group by initialization operation and form their own group key say Knew
b) Merge the new group to the old existing group.
c) To merge these two groups, sponsor(GC) of each group broadcasts their blind key to the all members of other group and form a new group key (x1.x2.P) just like as two parties key exchange. Where x1 , x2 are group secrets of old and new group respectively.
3 Leave Operations
If no. of leaving sensors is one or very few then it can be handle few times calling of single leave operation which require just one broadcast message. But if the no. of leaving sensors are very large then Mass Leave operation is perform which is suggest that it is better to reinitialize the tree with other than leaving members.

4.3.1 Single Leave:
In case of single leave, key path from the leaving member to the root of the tree must be updated. If the leaving member is group controller (GC) then choose some other member as the group controller but no need to change other subgroup controller. Leave operation in proposed protocol is very similar to that in TGDH. Suppose that we have n members in the group and assume that member Md leaves the group. First, each member updates its key tree by deleting the leaf node corresponding to Md. If Md have only one sibling, the former sibling of Md is promoted to replace Md's parent node. Leave operation in proposed protocol is very similar to that in TGDH .the sponsor generates a new key share, computes all {key & blind key contribution with others siblings} on the key-path up to the root, and broadcasts the Messages required to initialization of 'm' members + 2 new set of blind key contributions. This allows all members to compute the new group key. So there is only one round and only one message is require in leave operation. The no. of point

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

nCORETech 2017

LBS College of Engineering, Kasaragod

Vol. 6, Special Issue 3, March 2017

multiplication is depends on the location of the (n+ 3h-2) when the leaving node locates in deepest level. Note that the sponsor in this case is the rightmost leaf node of the sub tree rooted at the leaving member's sibling node.

4.3.2 Mass Leave:

If the no. of leaving members are very large then it is better to reinitialize the tree with other than the leaving members. So if n be the total no. of members in initial group and m is the no. of leaving members from current group then

The message cost of the mass leave operation is:

$$3\frac{(n-m-1)}{2}$$

Total no. of point multiplication is:

$$\frac{5(n-m-1)}{2}$$

Note that after numerous group operations like join, leave, mass join etc. the resultant key tree becomes quit unbalanced. So as suggested in when the key tree reaches a certain imbalance point, we should rebalance the tree and treat the rebalance operation as the group operation required. The imbalance point can vary depending on network and efficiency requirement. The proposed paper does not provide any new rebalancing scheme however protocol .Also sometimes it is more suitable to reinitialize the tree instead of rebalancing.

VI. AUTHENTICATION

Although the proposed protocol is based on elliptic curve Diffie Hellman which is secure and not easy to break, the entire system is vulnerable if the keys are not securely distributed. Therefore, we should implement an authentication algorithm in the protocol in wireless sensor networks. There are several ways to authenticate a group key exchange, such as centralized authentication, implicit authentication, and pairwise. In all operations of the protocol any of the above authentication schemes can be used.

VII.CONCLUSION

This paper gives a method for efficient contributory group key agreement protocol for wireless sensor networks. Here group is organized in a logical ternary key tree instead of binary tree. For key computation it uses ECC based three parties Diffie-Hellman based on GDH.2. The paper describes the implementation of major group key management operations in sensors.

REFERENCES

[1] An Efficient and Secure Key Establishment Scheme for Wireless Sensor Network Eric Ke Wang, Yunming Ye IEEE explore
[2] An Efficient Tree-Based Group Key AgreementUsing Bilinear MapSangwon Lee1, Yongdae Kim2, Kwangjo Kim1, and Dae-Hyun Ryu3
[3]. XIAOJIANG DU, HSIAO-HWA CHEN," SECURITY IN WIRELESS SENSOR NETWORKS" IEEE Wireless Communications
[4] Vikash Kumar, Anshu Jain and P N Barwal "Wireless Sensor Networks: Security Issues, Challenges and Solutions" International Research Publications House
[5] Madhumita Panda "Security in Wireless Sensor Networks using Cryptographic Techniques" American Journal of engineering Research
[6] SANJEEV KUMAR GUPTA, POONAM SINHA "Overview of Wireless Sensor Network: A Survey" www.ijarcce.com
[7] Chris Karlof David Wagner "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures"