International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 02, Issue – 03, March – 2017, PP – 69-74

Secure Key Pairing Transmission using Secret Agreement in Multi-hop Wireless Sensor Network

G. Roshini[1], S. Saravana Priya[2], C. G. Shrinidhi[3], Dr. K. Valarmathi[4] M.E.PhD

[1]*(Computer Science Department, Panimalar Engineering College, India)*
[2]*(Computer Science Department, Panimalar Engineering College, India)*
[3]*(Computer Science Department, Panimalar Engineering College, India)*
[4]*(Computer Science Department, Panimalar Engineering College, India)*

Abstract: With latest means for data transmission there arises a need to revise the security measure every often. Creating secrets from packet erasures again depends on information loss of legitimate nodes involved in the network. In order to avoid future loophole of security breach, we use secure key pairing transmission method using Secret Agreement Protocol and DSA (Digital signature algorithm) to bring effective advancements in multi-hop networks. This is done by signing and verifying (encryption and decryption) of data at sender and receiver side. Neighbourhood forwarding algorithm is used for establishing the communication path among mobile sensor nodes.

DSA helps in creating a network such that passive adversary can't even access the related information associated to transmitted data (original data), hence data becomes more reliable. Also it's exclusive for active adversary as it can't breach the security. Question & answer method is used between server and receiver to foster the security against active adversary and proxy mobile nodes if present. Thereby security measure of this paper will overcome the maximum threats in future as it involves a strong security process and it is feasible for wide range of network.

Keywords: neighbourhood forwarding algorithm, secure key pairing, active adversary, DSA, question & answer method.

1. Introduction

Consider a multi-hop wireless network, where confidential data has to be sent from a sender to receiver consisting of 'n' number of nodes, each of which acting as mobile sensor nodes in between. In unlimited network this data has to be transferred. Also in case of attack on signature by the adversary (active adversary), cryptosystem must be built such that data integrity is offered at its maximum in order to avoid plagiarism by business analysts and misusing the sender's identity for personal benefits or any illegal purpose.

Message authentication, data integrity, privacy and non-repudiation are important aspects of secrecy which has to be done efficiently and meet its need in Information security. Creating pairwise secrets depending on the data missed by legitimate nodes (sender and receiver) alone will not secure the system. From [1] we conclude that there is a need to create a secure key pairing for data transmission in multi hop which will be addressed in this paper:

Active adversary's attack: When an active adversary gets the access to data, the result will be far beyond just sniffing and getting the pirated details which is meant to be kept confidential.

Unlimited network: Attempts to enforce secrecy in large network capabilities were prone to attacks easily due to poor security guarantees [5],[10] and [11].This proves that even with unlimited network presence of adversaries(passive and active) also secrecy must be strong .

Duplication of mobile nodes: According to the secrecy capacities described by [9], it is proved that sender can send maximum rate of reliable data to receiver if the rate at which adversary or any mobile sensor nodes obtains at least an arbitrary amount of small information. This proves that adversary still has chance to access data. In order to overcome this flaw we use question and answer method for receiver and server, upon answering right only the key to get original data will be received. And each time this key varies for different data.

Thus pertaining to protocols used in [1] and implementing DSA (Digital Signature algorithm) an efficient cryptosystem to be used in application can be built. DSA performs signing and verifying process from sender and receiver side in order to provide authentication and data integrity. Thereby the adversary (active) in cryptosystem does not even get any related information about the original data transmitted using bootstrap information.

2. Existing System

The existing system [1] gives protocols for creating pairwise secrets in a group of wireless nodes with the presence of passive adversary, limited network presence and does not consider the computational and memory capabilities. It was built with the majority of results shown in [3], which says that information theoretic security is more desirable in cryptography than computation power as that does not require any assumption about enemy's computing power and justifying weaker security will be avoided. Criterion for perfect secrecy is often prejudged to be impractical because of the theorem given by Shannon [7] which states that:

In order to achieve perfect secrecy the secret key must be as long as plain text or:

H (K) >= H (M) (1)

Where, H (K) is the length of secret key and H (M) is the normal message. However attempts to prove this assumption by Shannon is wrong was backfired as the reasons made to substantiate this was unrealistic.(quantum cryptography and randomized cipher).Also he suggested that since majority of the ciphers are not built as given in (1),the secret key can be easily broken using exhaustive search.

There are two basic protocols used in [1] to prove that pairwise secrets are information theoretically secure.

2.1. Basic secret-agreement protocol in single hop.

It uses broadcast nature of wireless networks to create pairwise secrets between all pair of nodes simultaneously, agreeing to the polynomial time complexity, readily implementable in simple wireless device. It is based on the analysis that:

(i) It does not leak information to adversary.

(ii) The generation rate for secrecy is optimal for n=2

2.2. Secret agreement protocol for arbitrary, multi-hop.

(i) This is important mainly because if connection is disrupted then it will be challenging to maintain the single hop connected network.

(ii) It offers 2 ways for creating secrecy:

(a) Interference- Affects the reception of adversary but not other legitimate nodes involved.

(b) Multipath- Adversary located at any fixed position may not receive all packets of information and misses it through multipath propagation but the reception of legitimate nodes does not gets affected.

Multi-hop network also comprises some additional features apart from basic protocol. This includes the customised packet dissemination protocol that transfers data only to legitimate nodes and is decentralized.

Overall experimental evaluation proved that secret generation rate can be created in the magnitude of kb/sec independent from adversary's computational capacity compared to the previous works in [12],[13] which could generate bits/sec.

3. Proposed System

In the proposed system we generate a secure key pairing transmission in multi-hop network incorporating the secret agreement protocol and DSA for secured communication between sender and receiver. It mainly focuses on acting as a base for practical implementation. This is close to [6], which was the first to study the problem of secure data transmission on a multicast. But it was not information theoretically secure despite of being close for practical approaches. The work in [5] suggests a more theoretical model for security which addresses a lot practical requirements. When even small "meaningful information" is received by adversary then it becomes a step closer to guess the cipher text through randomization.

Thus by setting question and answer method for receiver and server we can detect the adversaries easily. Data integrity will be efficient in large network parameters for multi-hop. The signing- verifying process and question and answer method plays an exclusive role in addressing active adversary and out powers the existing system. Hence we reach a step close to practical implementation and it can be brought into existence in the near future.

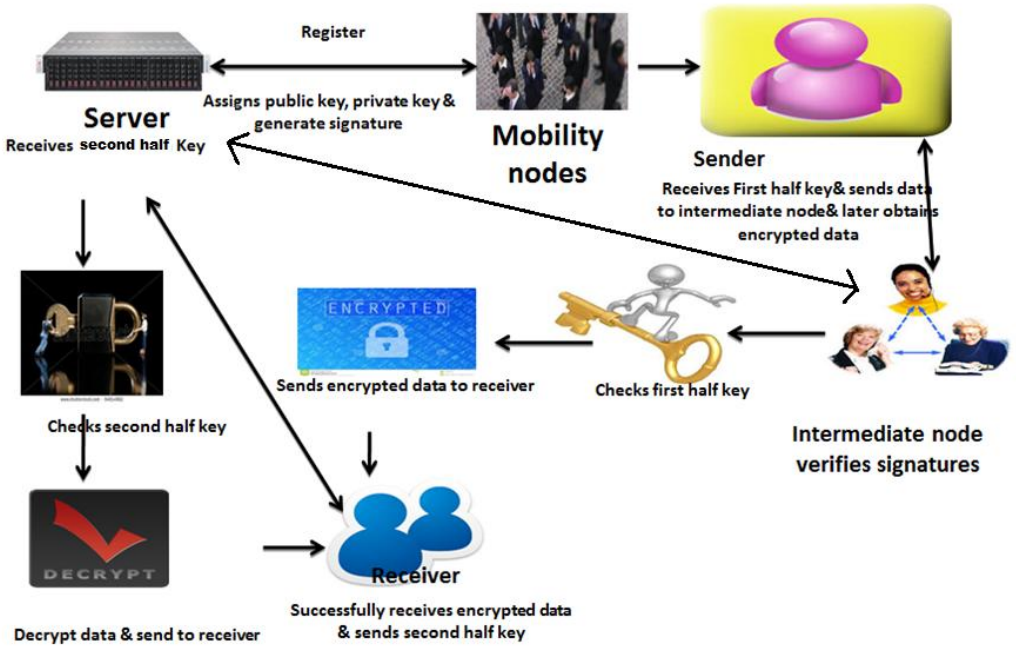

Fig. 1

Architecture diagram

According to the fig. 1 sender sends the data with the first half key to intermediate nodes. Intermediate nodes checks the signature generated by server to that of key sent by sender. If both match, source gets the encrypted data. As one of the key parts of signature is sent to the sender and other key part is sent to the receiver. Then sender sends encrypted data to receiver, receiver on receiving it sends the second half key to server. Then server checks the second half key and if matches with the signature it produced earlier, it decrypts the data and sends to receiver. There by receiver gets the decrypted data.

4. Modules and Overview

In the wireless sensor network 'n' numbers of mobile sensor nodes are available and each node communicates to nearest node for connection establishment. The sensor nodes are connected to the server and server assigns the node id, public key and private key. DSA (Digital signature algorithm) algorithm is used for generating signature (by combining the global public key and sender's private key).It is sent along the hash code& a random no. 'k' is generated for that particular signature . The sender sends the packet to the neighbouring node that has unique connection of +1 to be presented and again connect to another neighbouring node until it reaches receiver's location. If in any sensor nodes repetition occurs in the intermediate routing then remove that specific intermediate node connection and represent it as -1. So, +1 and -1 will be activated in the network using the neighbourhood forwarding algorithm in the wireless sensor environment.

4.1 Network Connection

Server monitors 'n' number of nodes. Then each node connects with the nearest node to establish their connection and it also monitors those bridge connections between nodes and server. The server monitors all the nodes and it shares their information like node id, public key and private key with each other mobile nodes. Sender requests neighbouring nodes based on covered area within required distance range. Then server covers and monitors the nodes under the certain region in the network.

4.2 Path Establishment

After establishing network connection, path has to be established. The server monitors all the nodes and it sends information like node id, public key and private key for all the mobile nodes present. Sender sends its RREQ (Route Request) in the network assigning the range up to which it can travel initially, after that it re-

broadcasts the RREQ to remaining nodes for the same distance until the data is sent. The receiver on receiving the RREQ sends its acknowledgement by RREP (Route Response) to sender, establishing the path.

4.3 Secure Packet Transmission from Server

Each node will be having the node id and other node details for sharing their packet to destination from the sender. Server assigns public and private keys for each node and do key pairing that is called signature. Key pairing is a process to generate a code by combining both keys and then splitting the signature. The server sends first half key of signature to sender and second half key to the receiver. Intermediate node on checking first half key with server and sender only gives the encrypted data to receiver. Also the second half key is checked by server directly and only then decryption takes place.

4.4 Signature

The signature of the message M will be a pair of the numbers r and s which will be computed from the following equations.

$r = (g^k \bmod p) \bmod q$

$s = (k^{-1}(H(M) + xr)) \bmod q$

k^{-1} is the multiplicative inverse of k (mod q). The value of H (M) is a 160-bit string which is converted into an integer according to the SHS standard. Then the signature is sent to the verifier.

4.5 Verification

Before getting the digitally signed message the receiver must know the parameters p, q, g, and the sender's public key "y". Let M′, r′, s′ be the received versions of M, r, and s. To verify the signature the verifying program must check to see that $0 < r' < q$ and $0 < s' < q$ and if either fails the signature should be rejected. If both of the conditions are satisfied then we will compute

$w = (s')^{-1} \bmod q$

$u_1 = [(H(M'))\, w] \bmod q$

$u_2 = ((r')\, w) \bmod q$

$v = (((g)^{u1}\, (y)^{u2}) \bmod p) \bmod q$

Test v=r'

4.6 Detecting attacker and alternate path selection

Proxy nodes may try to send or receive the data by attaching its second half key with the sender's first half key. These proxy nodes are called adversary (active adversary). It is detected by verifying the key pairing from the server. Those detected nodes are removed from the network and server track the receiver's address to choose the alternate path from the detected node position.

4.7 Question and answer and erasure technique

Data is encrypted and travels through selected path to reach receiver. At the same time all the data are stored in the server by using Erasure Code technique. So missed data can be retrieved by the help of erasure code technique from the server. Also, before receiver sends the second half key to server, question and answer is kept to the specified receiver for secure transmission. It must answer the server with correct answer. If any mismatch occurs it detects those specific nodes and removes and informs the server about that.

5. Related Work

According to [7], by Shannon a secret communication can be established between sender and receiver only if they both have common knowledge about the potential enemies. As this is practically challenging and relatable in the real world, it was revised in [8] stating secure communication can be achieved (computationally proved) even if just the receiver is aware of the threats not necessarily both or all the legitimate nodes. So [3] clearly states that perfect secrecy can take place even in a noisy channel provided error control code should be combined along with cryptographic coding to achieve virtually perfect secrecy. An upper bound of secrecy capacity and computational tightness are given in [4], for the models which adversary posses additional information called Wiretap Side Information(WSI), which are not available to legitimate terminals in the network .This is a special case to be considered.

A wiretap network model is introduced which uses information security with network coding to encode the information received from input links. From this wiretap network model, a group of channels in the network are given among which the wire tapper chooses one link to get information. This model includes the classical cryptography's concept. It constructs secure linear network code which controls the amount of information the

wire tapper receives on the message. This model is brought only in multicast network and its information theoretically secure. But the drawback faced in this model [6] is that the attempt to enforce strong security in large network was not great.

All this brings the need for creating a strong security with large network and active adversary's presence beyond just addressing the noisy channels and how to communicate securely in multi-hop. Also a cryptographic system should be information theoretically secure and practically feasible. Proving just one and leaving the other is not a good sign in information security.

6. Algorithms Used

6.1 DSA (Digital Signature Algorithm)

Signature and Verification process

DSA is based on the difficulty of computing discrete logarithms. This approach makes use of hash function. Hash code is provided as input to a signature function along with the random number 'k' generated for a particular signature. Signature function also depends on sender's private key (PR_a) & a set of parameters known to a group of communicating principals-called global public key (PU_g).

Result is signature consisting of two components labelled s and r.

At receiving end the hash code of the incoming message is generated. This plus the signature is input to a verification function. The verification function also depends on the global public key as well as the sender's public key (PU_a) which is paired with sender's private key. Output of the verification is equal to signature component r if signature is valid.

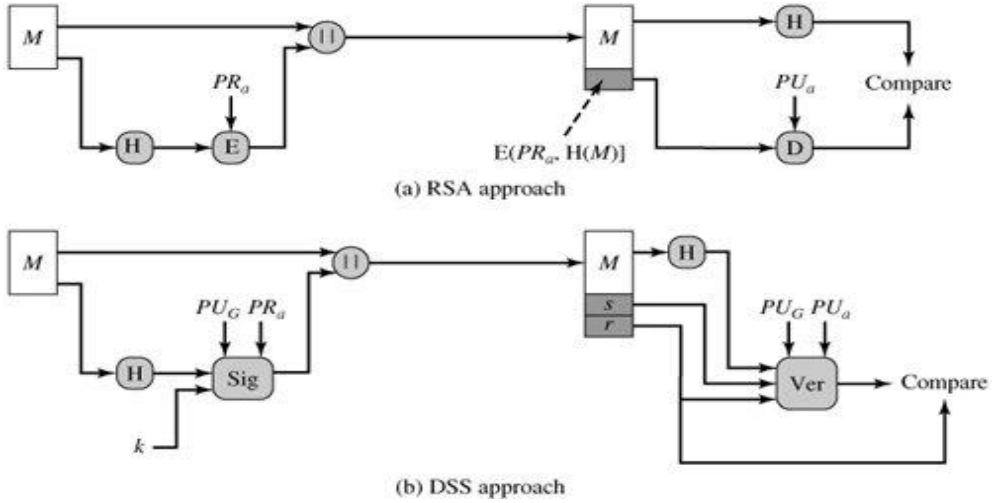

Fig. 2

Fig. 2 shows how why DSA is better than RSA. The general concept behind DSA is DSS (Digital Signature Standard approach).

Algorithm for DSA
Global key components

p=prime no. where $2^{L-1}<p<2^L$
for 512 <= L <= 1024 and L is a multiple of 64
q= prime divisor of (p-1), where
$2^{N-1} < q < 2^N$
g= h (p-1)/q mod p
Where h is any integer with 1 < h < (p-1)
Such that $h^{(p-1)/q}$ mod p > 1

User's private key
x = a randomly or pseudo randomly generated integer with 0 < x < q
User's public key
$y = g^x$ mod p

User's per message secret number
k = a randomly or pseudo randomly generated integer with $0 < k < q$.

6.2 Neighbourhood Forwarding Algorithm

In the network, from sender - xs(t) and the neighbour nodes 'n'.
Initialize list of neighbour nodes from 1 to n
For each node i in the network so comprised:

1. Calculate distance ($x_s(t)$, $x_i(t)$).
2. If ($x_s(t)$, $x_i(t)$ < Maximum distance which is set, choose the maximum distance up to which nodes can travel and keep forwarding.
   Where $x_s(t)$ is the starting distance of sender and $x_i(t)$ is the intermediate nodes present.

3. Connect the path chosen to establish the connection with destination.
4. Remove disconnected path which is repeated by indicating -1 and add the established path with +1.

Once RREQ reaches destination it will give ACK and precede the RREP.

7. Conclusion and Future Enhancement

A cryptosystem close to practical implementation and information theoretical conditions is built. In a wireless network consisting n nodes, with unlimited network capacities, proxy node attacks and presence of passive adversary; transmission of data between sender and receiver will be highly secure by using boot strap information. And probability of adversary trying to get any related information will also be negligible. The active adversary can't breach the security as the question and answer method is kept between receiver and server. Upon its confirmation only full data will be given to receiver.

As this model aims in bringing it close to real time application this can be implemented in banks and other high end requirements for security purposes.

Refernces

[1]. Iris Safaka, Laszlo Czap,Katerina Arygyraki, and Christina Fragouli, "Creating Secrets Out of Packet Erasures" IEEE,2016
[2]. A.D.Wyner,"The wire-tap channel",Oct-1975
[3]. U.M.Maurer,"Secret key agreement by public discussion from common information",IEEE. May 1993
[4]. I.Csiszar and P.Narayan,"Secrecy capacities for multiterminal channel models",IEEE.Jun-2008
[5]. K.Bhattad and K.R.Narayanan"Weakly secure network coding ".Apr-2005
[6]. N.Cai and R.W.Yeung,"Secure network coding schemes on wiretap network".IEEE-Jan 2011.
[7]. "Communication theory of secrecy systems".Oct 1949
[8]. W.Diffie and M.E.Hellman,"New directions in cryptography".IEEE Nov 1976.
[9]. I.Csiszar and J.Korner,"Broadcast channels with confidential messages".IEEE,May 1978
[10]. Y.Wei,Z.Yu and Y.Guan,"Efficiently Weakly secure network coding schemes against wiretapping attacks".IEEE-Jun 2010.
[11]. M.Adeli and H.Liu ,"On the inherent security of linear network coding".IEEE Aug 2013
[12]. C.Ye.S.Mathur ,A.Reznik,Y.Shah,W.Trappe and N.B.Mandayam,"Information theoretically secret key generation for fading wireless channels",IEEE.June 2010.
[13]. H.Liu,Y.Wang,J.Wang,Y.Chen,"Fast and practical secret key extraction by exploiting channel response".Apr-2013.

