Secure Data Transmission with Hierarchical Clustering

Rahul Raj[1], J. Godwin Ponsam[2]

[1]Master of Technology, SRM University, Faculty of Engineering and Technology,
Kattankulathur 603203, Kancheepuram, Tamil Nadu, India.

[2]Assistance Professor (Sr.G), Dept. of IT, SRM University, Faculty of Engineering and Technology,
Kattankulathur 603203, Kancheepuram, Tamil Nadu, India.

Abstract: ***Security in wireless sensor networks is currently provided exclusively through symmetric key cryptography. In this paper we show that the implementations of traditional cryptography is not enough to provide complete secure transmission over the wireless sensor networks. Here, we are going to discuss the drawbacks of the conventional way of routing and try to implement the Asymmetric key cryptography with few enhancement of using alternate sensor node in hierarchical clustering. The combination of IBS signature with multi-hop planner model in hierarchical clustering helps in reducing the impact of frequent node dies and its causes.***

Keywords: ID-Based Digital Signature, Secure data transmission protocol, Alternate sensor node, Cluster Hierarchy.

1. Introduction

A wireless sensor network is a collection of spatially distributed sensor nodes largely deployed in harsh and adversarial area for certain application such as military domain, sensing tasks with trust less surroundings to monitor physical and environmental conditions such as sound, motion temperature etc.

Each individual sensor nodes are capable of sensing their environments, processing the data locally and sending the data to one or more collection points within the WSN.

In cluster based wireless sensor network, the formation of cluster consists of a leader cluster head (CH) and non-CH leaf node. Each CH of each cluster aggregates the data collected by the leaf node in its cluster, and sends the aggregation to the base station (BS).

Different protocols are employed to the cluster network like LEACH or LEACH like protocol such as APTEEN or PEACH, but each having some drawbacks, a trade-off between energy efficiency and security implementation. Also, few other security protocols such as Sec-LEACH, GS-LEACH, and RLEACH are implemented in WSNS, but each using symmetric key management for security which suffer so called orphan node problem.

The use of public key can be a solution for such threat, the ID based signature for signing and verification for each sensor node protect the data from being compromised by the adversaries. Moreover adversaries are now using complex attack to compromise the wireless channel or node so it need an implementation of hard cryptographic algorithm. The Diffie-Hellman could be a solution for this whose hardness lies in the difficulty of computing discrete logarithms.

A number of attack can be possible in the network, which are characterize into active attack, passive attack, and node compromising attack. All such attack any how decrypt the captured data easily, so in order to provide strong encryption mechanism, the concrete ID-based encryption based on DHP (Diffie-Hellman problem) can be implemented to countermeasure these attack.

Also, in order to transmit the data from one node to different other node within a network an efficient routing algorithm is necessary when clustering is in use which some time suffer from black hole occurs when intermediary node relay huge amount of data through it, so there need an alternate option i.e. another sensor node which can take charge of it to avoid extra energy depletion. Then ASN algorithm can be helpful which depends on the capable neighboring nodes to relay the data further to next layer in the hierarchical cluster.

2. Objective

To develop an efficient routing algorithm which transmit the aggregation through hierarchical clusters securely in large-scale CWSN, by mitigating the existing protocol’s problem and to provide the efficient solution.

Scope: Usually, Sec-LEACH protocol suffers from many security issues such as orphan node problem, due to symmetric key mechanism which can be checked by public key cryptography. Also, the introduction of DHP and DLP can check the computational overhead and security concern of this model. Lastly, the implementation of ASN in multi-hop planner model mitigate the effect of self-induced black hole problem.

3. Literature Survey

3.1 Sec-LEACH — on the security of clustered sensor networks.

They proposed a security LEACH a modified version of LEACH that applies random key pre distribution to provide a baseline security. This protocol primarily focused to prevent energy drainage of a restricted set of CHs. As LEACH randomly rotates CHs among all nodes in the network from time to time thus distributing aggregation. Also, it assure the energy efficiency up to 8 times than other similar protocols.

Like any other routing protocol the LEACH is also vulnerable to a number of security attacks including jamming, spoofing, replay etc. However leach is more robust against inside attack than most other routing protocols, and all because of existing key distribution schemes are inadequate.

The Sec-LEACH, however, provides a random key pre-distribution schemes using symmetric key algorithm, in which a set of keys drawn from a much larger key pool is assigned to each node This algorithm does not have optimizations. It primarily focuses on how to secure the transmission. However with the increases in the different types of attack the use of symmetric key is no more helpful or secure the transmission from complicated attacker. Constraints related to node which limit the number of key sharing, energy efficiency memory processing makes it little unreliable to the threat.

However, this algorithm efficient enough to provide a base line security. Furthermore, the algorithm is manageable depending upon the critical aspect of the system, take into consideration, this protocol is a trade-off between two or more node constraints

There are two problems related to this protocol. One is orphan node problem, which doesn’t allow the node to either select the cluster or elect itself as a cluster increasing the overall energy consumed by the network. The use of asymmetric key for authentication and signing absolutely mitigate the current problem.

3.2 An authentication framework for wireless sensor networks using identity based signatures.

They propose an efficient and secure framework for authenticated broadcast\multicast by sensor node as well as for outside user authentication, which uses identity based cryptography online and offline signature schemes.

In this framework, the authentication process is divided into three categories, namely, base station to sensor node, sensor node to sensor node, and outside users to sensor node. All this provide a better effort to tackle the authorization process before transmission initiated. Practically, it first enables all the sensor node in the network to broadcast and/or multicast an authenticated message quickly, secondly to verify the message sender and the contents, and finally to verify the legitimacy of an outside user.

Authentication is a crucial security requirement to avoid attacks against secure communication, and to mitigate DoS attacks exploiting the limited resources of sensor nodes. But resource constraints of sensor nodes are hurdles in applying strong public key cryptographic based mechanism in WSNs.

This framework provides several features. Its ID-base signature i.e. IBS consists of four algorithm starting from system setup to key extraction followed by signature generation and verification. The same is for IBOOS schemes with additional online and offline signing instead of signature generation in IBS. Both of these protocol provides better framework to authenticate the user.

The advantaged in this protocol is the quick authentication broadcast and user authentication implemented by ID based signature schemes which can be re-use for security and performance improvements.

Few problems related to this framework, despite of being quick authentication broadcast it took time to the signing process and key establishment due to complex computation. So if it is used in some military domain, during war, the delay may prove a havoc to the situation. However, it is relatively easy to extend this algorithm to handle secure data transmission through hierarchical clusters, providing a framework for the SET.

3.3 A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature.

The use of ID-based signature in CWSN provides an efficient protocol for communication, by achieving all the security requirements for routing protocols. In this protocol the CH are selected as same as in the LEACH Protocol and hence are known as LEACH like protocol. But when it comes to security all the protocols using symmetric key as key distribution makes practically challenging as the dynamic clustering of nodes makes the trust relationship inadequate. Furthermore, these methods are specifically tailored for the problem of simple security concern, and cannot easily be adapted for more complicated one.

It uses a Diffie-Hellman algorithm as a traditional certificate-based cryptography that performs node to node pairing. The purpose is to derive an entity’s public key from the identity i.e. ID number. It uses pair wise similar information and takes advantage new insight into pruning the pattern. It is the pair wise similarity between instances. The similarities can be used to initiate the communication between the nodes.

In this works approach the protocol is divided into two phases, same as LEACH, the setup phase and the steady state phase for each rounds and in each frame the sensor nodes transmit the data to its CH, where each sensor nodes determines a random number and compares it with the threshold with the current round.

The disadvantage in using this protocols is extra energy consumption during the computation, increasing the overall energy consumption of the network and leads to dying of nodes soon.

However, such protocol provides a secure transmission throughout the network against complex attacks like sinkhole, wormhole, selective forwarding attack and many others due to the implementation of Diffie-Hellman algorithm which uses asymmetric key cryptography.

This extension can be included to the SET algorithm for securing the transmission with hierarchical clustering.

3.4 Efficient online/offline identity-based signature for wireless sensor network

The online/offline ID-based signature is an efficient way to decrease the cost of computational overhead suffered by clustered based wireless sensor networks. As the storage and computational cost for the severely constrained resources in WSN environment is high due to symmetric key algorithm, the counter algorithm based on public key cryptography can tackle the problem and provides an efficient ID-based signature in both online and offline mode. Practically, it severely reduces the cost of computation and storage due to the few modification, as follow, in the offline/online signature.

- No requirement for the certificate for verification.
- Re-usability of the offline pre-computed information.
- One time use of all the previous online\offline signature schemes.
- No requirement of the secret key information and can be pre-computed by PKG.

- Eliminating any communication between the sensor node and base station for the offline signing, which is considered as a costly factor in the WSN.

The advantage in this protocol is that it provides concrete ID based settings with 50% saving in computational and storage cost and have only two pairing operations in signature verification and else are already pre-computed by PKG (Public Key Cryptography).

This schemes shows how a single nodes sign multiple message through aggregation which again reduces the communication overhead in the network which is crucial for resource-constrained sensor nodes.

The only disadvantage in this schemes is, due to resource constrained, the lightweight devices may not be able to execute such operation.

The key idea for the success of this schemes is the removal of unwanted pairing and reusability of the pre-computed information and the aggregation of the message in the node.

However, for the extension this schemes is particularly suitable for large scale networks such as hierarchical cluster-based wireless sensor networks.

3.5 A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks.

The transmission of the data in CWSN is not always as simple, clusters are there to aggregate and process the data before transmission to base station, but when a large amount of nodes deployed in the environment it is unachievable that each sensor nodes can have direct communication to base station due to the constrained transmission range of transmitting equipment, the solution to this problem is the use of multi-hop planner model, in which CH transmits data to the base station by forwarding its data to one of its neighbor using alternative sensor node algorithm.

This algorithm is robust to non-uniform distributed sensor nodes and scales to larger amounts of spatially distributed nodes than that specified in the original challenge. A probabilistic estimate suggests that it may reduce the effect of self-induced black hole problem in multi-hop data gathering transmission.

Here in this algorithm after hierarchicalize sensor nodes into different levels using the hop number of transmissions to the base station. CH are selected autonomously and communicate with the base station using multi hop transmission which employ multi-hop planner model whereas non-CH sensor nodes communicate with sensor nodes directly. In this model both CH sensor nodes and non-CH sensor nodes could act as the intermediary node for data forwarding in routing.

The key idea behind the alternative sensor node routing is first introduce the state of the sensor node and then turn the particular sensor node into ASNs. This way prolonged the network lifetime and prevent the sudden death of a sensor node. And helps in reducing the effect of self-induced black hole problem.

The only disadvantage to this algorithm is that it could not completely remove the black hole problem, although, it could mitigate the effect caused by that, prolonging the network life time and also prevent the sudden death of sensor node.

4. Functional Requirements

The purpose of this project is to establish a secure communication channel for transmitting sensed data from cluster to base station for a large set of sensor nodes with in a network.

To fulfil such requirement following methods were adopted:

For the formation of the clusters the LEACH technique could be used for its dynamic and random way to nominate the Cluster Head, balancing the energy consumption for each node by periodically changing the CH for each round of cluster formation.
After the formation of cluster the sensor node is allowed to sensed and transmit the data to its cluster head where the CH processed the data locally, and after that only meaningful data is then send to the base station.

During the data transmission, there is a need for security protocol to avoid the complex attack at the wireless channel. Simple attack can be mitigate by simple algorithm, bur for the complex one the implementation of Diffie-Hellman problem as ID-based signature can completely secure the transmission against known possible attacks.
Also the key pairing and verification requires a lot of computation at each node, hence to reduce such computational overhead the Discrete Logarithm problem can

be implemented with ID-based Online\Offline signature.

After the establishment of the secure wireless channel between the sensor nodes to cluster head and up-to base station, a routing algorithm is required to form a path in a large-scale networks, a multi-hop planner model provides a better approach to this implementation.

The ASN algorithm helps in mitigating the effect of self-induced black hole problem. And also allow the neighboring node to carry the data forward to the base station through multi-hops.

5. Proposed Solution

Secure Data Transmission with Hierarchical Clustering

A proposal of SDT with hierarchical clustering is a multi-hop based algorithm that provides security to data on transit against well-known complex attacks. To counter measure the frequent attack the protocol has been modified to build on the hardness of these two algorithm.

- Diffie-Hellman problem.
- Discrete logarithm problem.

Also for efficient routing in hierarchical cluster the following modal has been adopted.

- Alternative sensor node algorithm.

We have to find the sequences with sub partition. This method is primarily focused at finding pairs (or sets) of motifs that co-occur in the data set within a short distance of each other. This method only considers a simple mismatch based definition of noise, and does not consider other more complex motif models. This model provides the calculation of number of mismatches.

Modules: A total of three modules have been designed.

Implementation of Diffie-Hellman Concept

- Generation of encryption key K for the homomorphic encryption schemes to encrypt data messages.
- Generation of pairing parameters which includes two prime numbers.
- Random input of any integer as a master key.
- And preload every node with the pairing parameters.

Algorithm for Diffie-Hellman

- Two public parameter p and q, where p is the prime number and q is the primitive root of p.
- Let node A and node B wish to exchange a key:
- Node A pick random integer XA < p and computes.

  $$Y_A = q^{X}{}_{A} \text{ (mod p)}$$
- Similarly for node B, XB < p and computes

  $$Y_B = q^{X}{}_{B} \text{ (mod p)}$$
- Each side keeps the X value private and makes the Y value available publicly to the other side
- Now each other side will compute the key as

  $$K = (Y_B)X_A \text{ mod p for node A.}$$
- And as

  $$K = (Y_A)X_B \text{ mod p for node B.}$$
- And two calculations will produce identical results.

  $K = (Y_B)\ X_A$ mod p
  $(q^{X}{}_{B}$ mod p$)\ X_A$ mod p
  $(q^{X}{}_{B})\ X_A$ mod p
  $(q^{X}{}_{A})\ X_B$ mod p
  $(q^{X}{}_{A}$ mod p$)\ X_B$ mod p
  $(q^{X}{}_{A}$ mod p$)\ X_B$ mod p
  $(Y_A)X_B$ mod p
- Hence the secret key have exchanged between the two nodes.
- Further, because XA and XB are private and adversaries has only following ingredients i.e. parameters p, q, YA and YB.

Thus, the adversaries are forced to take a discrete logarithm to determine the key, in the following way:

$$X_B = d\ \log_{p,\ q}(Y_B)$$

- The hardness of Diffie-Hellman lies in the fact that it is easy to calculate the exponential modulo a prime, but it is very difficult to compute the discrete logarithm.

Implementation of Discrete Logarithm Problem

- To make the security a little harder to compromise, the discrete logarithm problem could be implemented, which is fundamentally is defined to be a power to which some positive base must be raised in order to equal the number. i.e. for base x and for value y:

  $$X = X^{\log_{x}(y)}$$
- The properties of logarithms include a primitive root a for some prime number p.
- So, by the definition of modular arithmetic, it follow that for any integer b and a primitive root a of prime number p, we can find a unique exponent i such that the following equation holds:

  $$b = a^{i} \text{ (mod p),}$$

  Where, 0 <= i <= (p-1)
- Steps in discrete logarithm problem:
- Take a prime number p and computes x and y, such that:

  $X = a^{d\log_{a,p}(X)}$mod p,
  $Y = a^{d\log_{a,p}(Y)}$mod p,
  $XY = a^{d\log_{a,p}(XY)}$mod p.
- Applying the rule for modular multiplication:

  XYmod p = [(X mod p)(Y mod p)]mod p,
  $a^{d\log_{a,p}(XY)}$ mod p = $[(a^{d\log_{a,p}(X)}$mod p$)(\ a^{d\log_{a,p}(Y)}$ mod p)]mod p,
  $= [a^{d\log_{a,p}(X)+d\log_{a,p}(Y)}]$mod p
- Now by Euler's theorem, for every a and n that are relatively prime,

  a.φ(n) = 1 (mod n).
- So, by Euler's theorem,

  $a^{z} = a^{q}$ (mod n), if z = q (mod φ (n)).
- Then, d $\log_{a,p}(XY) = [d \log_{a,p}(X) + d \log_{a,p}(Y)]$ (mod φ(n)).
- The hardness of discrete logarithm mod 'p' to some base 'a' exist only if 'a' is a primitive root of 'p'.

Further, not every number has the primitive root, a few in integer makes the assumption for adversaries quite hard.

Use of Alternative Sensor Node Algorithm

- The alternative sensor node is used for routing purpose, in order to reduce the effect of self-induced black hole problem.
- For any node in between the transmission range of others node the distance threshold value helps in determining the route for the transmission, which can be decided by the transmission range of the node.
- For too large or too small value of distance threshold the routing will not be feasible.

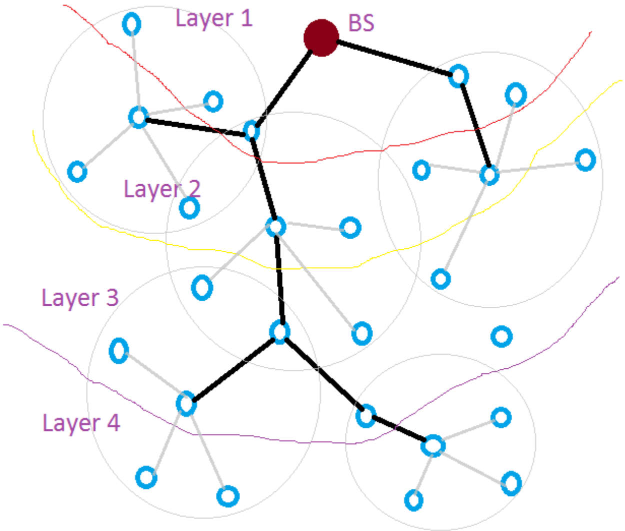

Figure 1: Data Transmission in ASN model.

Algorithm for the alternative sensor node

(Divided into five steps for each round.)

- Counting hope number: To count the hop number of the sensor node and maintain the routing table for each route in its memory.
- Hierarchicalizing sensor nodes: Organize the sensor node according to their hop number in layers starting form base station.
- Clustering in the system: Using the LEACH method the clusters are formed depends on the threshold value for a node to become cluster head (CH):

$$T (n) = P / (1-P*(r \bmod [1/p])),$$

Where, p is the desire percentage of CH during a round, r is the current round number n is the node that have not been CH nodes in the last [1/p] rounds.

For each layer, the CH will mark as $\text{level}_n\text{CH}_n$ for identification.

And the non-CH will join the cluster using 1 hop communication, which depends on the strongest transmission signal.

- Transmission and scheduling in clusters: all the CH node are scheduled in TDMA medium access control to avoid collision.
- Selecting transmission routes:
- Select the smallest hop number,

$H_{route} = \text{Min}\ \{H_i\}$

- Select the route with the highest energy node among the lowest energy node,

$E_{route} = \text{Max}\ \{\text{Min}\ \{E'_{i\,j}\}\},$

Where, $E'_{i,j}$ is the energy of the lowest energy node j in route i.

- After establishing the route for transmission, discover the alternative sensor node while transmitting data.
- So, if there exist an alternative node ASN n (say Nalt) for a sensor node m near its transmission route, then the sensor node m stops its routing function and let node n take charge in the route.

$N_{alt} = \{\text{exist} \mid (S_{mn} < R/2) \wedge (E_n > E_m)\},$

Where, S_{nm} is the distance between two sensor nodes, E is the energy of a sensor node, and R is the transmission range for a sensor node.

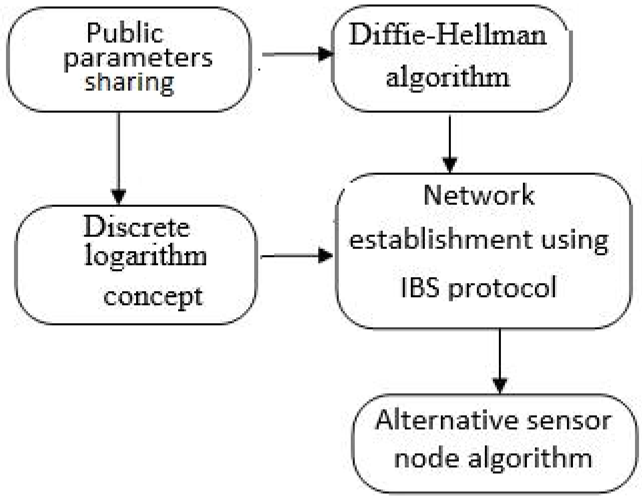
Public parameters sharing
Diffie-Hellman algorithm
Discrete logarithm concept
Network establishment using IBS protocol
Alternative sensor node algorithm

Figure 2: Architecture of proposed system.

6. Conclusion

In this paper we have provided few issues of using symmetric key mechanism as implementations particularly at wireless sensor networks for routing purpose. We have shown that the use of sec-LEACH and other related protocol which is not sufficient to tackle the complex attack and the ultimate result is the loss of connectivity to a node. The proposed solution can actually reduce the amount of traffic over-head due to key management in WSN. The computational cost is within acceptable limits and sufficiently fast. And finally it will provide the WSN the secure way of routing with clustering hierarchy using multi-hop planner model by forwarding its data to its neighboring node using the ASN algorithm.

References

[1] L.B. Oliveira et al., “Sec-LEACH-On the Security of Clustered Sensor Networks,” Signal Processing, vol. 87, pp. 2882-2895, 2007

[2] R. Yasmin, E. Ritter, and G. Wang, “An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures,” Proc. IEEE Int’l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.

[3] H. Lu, J. Li, and H. Kameda, “A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature,” Proc. IEEE GLOBECOM, pp. 1-5, 2010.

[4] J. Liu et al., “Efficient Online/Offline Identity Based Signature for Wireless Sensor Network,” Int’l J.

Information Security, vol. 9, no. 4, pp. 287-296, 2010.

[5] H. Lu, J. Li, and G. Wang, “A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks,” Proc. Fourth Int’l Conf. Frontier of Computer Science and Technology (FCST), pp. 565-570, 2009.

[6] Huang Lu, Jie Li, and Mohsen Guizani, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014.

Author Profile

Rahul Raj Pursuing M.Tech degrees in Information Security and Cyber Forensics from SRM University, Chennai. Under the Guidance of **Prof. J Godwin Ponsam** (Dept. of IT) SRM University, Chennai**.** India