Enhancing the Security in WSN using Three Tier Security Architecture

Chanchal G. Agrawal\(^1\)  
SCOE, Pune University

Prof. J. B. Kulkarni  
SCOE, Pune University

Abstract— Security is the main issue while setting up the WSN network for node communication. This report describes the efficient mechanism for achieving the security between node communications by creating three tier security architecture. This system implements three tier architecture with the use of two polynomial pools having sensor nodes, mobile sinks and some access points that are also sensor nodes, to get better security. Two pools are common mobile polynomial pool and common static polynomial pool. Mobile sinks and access point carries keys from common mobile polynomial pool were as, access points and sensor nodes carries keys from common static polynomial pool. Communication gets established from mobile sink to access point then from access point to sensor node that shows three tier architecture Authentication is the main aspect of the system, that is achieved by pairwise key predistribution methods and authentication of the nodes with the use of polynomial keys. Here, Mobile sink replication attack is implemented against the network. The malicious node, it is blocked. If it wants to communicate within the network then it needs to capture large no of keys from both the pools for authentication. But as the sufficient keys are not available with it, it cannot communicate with the other nodes in the network.

Keywords— Wireless Sensor Network, Random key predistribution, Mobile Sink, Common Mobile Polynomial, Common Static Polynomial.

I. INTRODUCTION

In electronic technology recent advanced have paved the way for the development of a new generation of wireless sensor networks (WSNs) consisting of a large number of low-power, low-cost sensor nodes that communicate wirelessly. Such sensor networks can be used in a wide range of applications, such as, military sensing and tracking, health monitoring, data acquisition in hazardous environments, and habitat monitoring. The sensed data often need to be sent back to the base station for analysis. However, when the sensing field is too far from the base station, transmitting the data over long distances using multi hop may weaken the security strength (e.g., some intermediate may modify the data passing by, capturing sensor nodes, launching a wormhole attack, a Sybil attack, selective forwarding, sinkhole, and increasing the energy consumption at nodes near the base station, reducing the lifetime of the network. Therefore, mobile sinks (MSs) (or mobile soldiers, mobile sensor nodes) are essential components in the operation of many sensor network applications. The Proposed system {Security in WSN using polynomial pool based mechanism} “is the combination of two pools. This scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single polynomial from the mobile pool to gain access to the network for the sensor’s data gathering. Polynomials from the static polynomial pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access node.

II. RELATED WORK

An Wireless sensor networks are one of the first real world examples of pervasive computing, the notion that small, smart and cheap sensing and computing devices will eventually permeate the environment [8]. Wireless sensor network (WSN) consists of a large number of ultra small sensor nodes. Each sensor node is an autonomous battery operated device with data processing capabilities, integrated sensors, limited memory and a short range radio communication capability. In application scenarios sensor nodes are randomly deployed over a region and collect data.

Wireless Sensor Networks are deployed for a wide variety of applications like military tracking, monitoring of environment, smart environments, patient tracking, etc. [1]. Security is extremely important when sensor nodes are deployed in hostile environments because they may be exchanging valuable or critical information about the environment and an adversary can use this information to his advantage or inject malicious information into the network. Apart from physical capture a malicious user can easily tap into the wireless communication and listen to the traffic, inject misleading data into the network or impersonate as a node of the network. To provide security, encrypted and authenticated communication is required. Active research is being pursued for efficient setup of secure keys in wireless sensor networks. Setting up of keys for secure communication is a part of the Key Management problem.

In general network environments there are three types of key agreement schemes: trusted server scheme, self enforced scheme and pre-distribution scheme. The trusted server scheme has a trusted server between two nodes to negotiate a shared key between the nodes. This scheme is not feasible in sensor networks because there is no central server in most WSN. Self enforcing scheme uses public key algorithms such as Diffie-Hellman key agreement or RSA. Pre-distribution scheme uses secret keys to establish pairwise keys after they are deployed.

In the new security framework, a small fraction of the preselected sensor nodes (see Fig. 1), called the stationary access nodes, act as authentication access points to the network, to trigger the sensor nodes to transmit their aggregated data to mobile sinks.

© 2014, IJIRIS- All Rights Reserved
A mobile sink sends data request messages to the sensor nodes via a stationary access node. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Using two separate key pools and having few sensor nodes that carry keys from the mobile key pool will make it more difficult for the attacker to launch a mobile sink replication attack on the sensor network by capturing only a few arbitrary sensor nodes. Rather, the attacker would also have to capture sensor nodes that carry keys from the Mobile key pool. Keys from the mobile key pool are used mainly for mobile sink authentication, and thus, to gain access to the network for data gathering.

Although the above security approach makes the network more resilient to mobile sink replication attacks compared to the single polynomial pool-based key predistribution scheme [14], it is still vulnerable to stationary access node replication attacks. In these types of attacks, the attacker is able to launch a replication attack similar to the mobile sink replication attack. After a fraction of sensor nodes have been compromised by an adversary, captured static polynomials can be loaded into a replicated stationary access node that transmits the recorded mobile sink’s data request messages to trigger sensor nodes to send their aggregated data.

To make the three-tier security scheme more robust against a stationary access node replication attack, also strengthened the authentication mechanism between the stationary access nodes and sensor nodes using one-way hash chains algorithm [2] in conjunction with the static polynomial pool-based scheme [1].

Pairwise key establishment is another important fundamental security service. It enables sensor nodes to communicate securely with each other using cryptographic techniques.

The main problem is to establish a secure key shared between two communicating sensor nodes. However, due to the resource constraints on sensor nodes, it is not feasible for them to use traditional pairwise key establishment techniques such as public key cryptography and key distribution center (KDC).

Eschenauer and Gligor proposed a probabilistic key pre-distribution scheme recently for pairwise key establishment. The main idea is to let each sensor node randomly pick a set of keys from a key pool before the deployment so that any two sensor nodes have a certain probability to share at least one common key. Chan et al. further extended this idea and developed two key pre-distribution techniques: a q-composite key pre-distribution scheme and a random pairwise keys scheme. The q-composite key pre-distribution also uses a key pool but requires that two nodes compute a pairwise key from at least q predistributed keys that they share. The random pairwise keys scheme randomly picks pairs of sensor nodes and assigns each pair a unique random key. Both schemes improve the security over the basic probabilistic key pre-distribution scheme.

However, the pairwise key establishment problem is still not fully solved.

For the basic probabilistic and the q-composite key pre-distribution schemes, as the number of compromised nodes increases, the fraction of affected pairwise keys increases quickly. As a result, a small number of compromised nodes may disclose a large fraction of pairwise keys and also achieves significant security under small scale attacks at the cost of greater vulnerability to large scale attacks.

Though the random pairwise keys scheme does not suffer from the above security problem, given a memory constraint, the network size is strictly limited by the desired probability that two sensor nodes share a pairwise key, the memory available for keys on sensor nodes, and the number of neighbor nodes that a sensor node can communicate with.

The problem of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. For the basic probabilistic and q-composite key pre-distribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of the network sensor nodes, making it possible for the attacker to take control of the entire network by deploying a replicated mobile sink, preloaded with some compromised keys to authenticate and then initiate data communication with any sensor node.

© 2014, IJIRIS- All Rights Reserved
There is a tradeoff to be made between security and vulnerability that has to be considered based on the sensor network size and application.

The proposed scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single polynomial from the mobile pool to gain access to the network for the sensor’s data gathering. Polynomials from the static polynomial pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes. Prior to deployment, each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool. In this scheme, to improve the network resilience to mobile sink replication attack as compared to the single polynomial pool based approach, intend to minimize the probability of a mobile polynomial being compromised if Rc sensor nodes are captured. As an adversary can use the captured mobile polynomial to launch a mobile sink replication attack, achieve this by having a small fraction of randomly selected sensor nodes carry a polynomial from the mobile polynomial pool. These preselected sensor nodes are called the stationary access nodes. They act as authentication access points for the network and trigger sensor nodes to transmit their aggregated data to the mobile sinks.

A mobile sink sends data request messages to the sensor nodes via a stationary access node. The mobile sink’s data request messages will initiate the stationary access node to trigger sensor nodes to transmit their aggregated data to the requested sink. Each stationary access node may share a mobile polynomial with a mobile sink. All sensor nodes, including the stationary access nodes, randomly select a subset of polynomials from the static polynomial pool. The advantage of using separate pools is that mobile sink authentication is independent of the key distribution scheme used to connect the sensor network. This scheme is divided into two stages: static and mobile polynomial predistribution and key discovery between a mobile sink and a sensor node.

- Static and mobile polynomial predistribution:
  Stage 1 is performed before the nodes are deployed. A mobile polynomial pool \( |M| \) of size \( |M| \) and a static polynomial pool \( S \) of size \( |S| \) are generated along with the polynomial identifiers. All mobile sinks and stationary access nodes are randomly given \( K_m \) and one polynomial (\( K_m > 1 \)) from \( M \). The number of mobile polynomials in every mobile sink is more than the number of mobile polynomials in every stationary access node. This assures that a mobile node shares a common mobile polynomial with a stationary access node with high probability and reduces the number of compromised mobile polynomials when the stationary access nodes are captured. All sensor nodes and the preselected stationary access nodes randomly pick a subset of \( K_s \) and \( K_s - 1 \) polynomials from \( S \). Fig. 2 show the key discovery between the mobile node and stationary node.

- Key discovery between mobile node and stationary node:
  To establish a direct pairwise key between sensor node \( u \) and mobile sink \( v \), a sensor node \( u \) needs to find a stationary access node \( a \) in its neighborhood, such that, node \( a \) can establish pairwise keys with both mobile sink \( v \) and sensor node \( u \). In other words, a stationary access node needs to establish pairwise keys with both the mobile sink and the sensor node. It has to find a common mobile polynomial with the mobile sink and a common static polynomial with the sensor node. To discover a common mobile/static polynomial, a sensor node \( i \) may broadcast a list of polynomial IDs, or alternatively, an encryption list \( a, EK_v(a), v = 1, \ldots, |K_s| \), where \( K_v \) is a potential pairwise key and the other node may have as suggested in [12] and [13].
When a direct secure path is established between nodes \( u \) and \( v \), mobile sink \( v \) sends the pairwise key \( K_c \) to node \( a \) in a message encrypted and authenticated with the shared pairwise key \( K_v,a \) between \( v \) and \( a \). If node \( a \) receives the above message and it shares a pairwise key with \( u \), it sends the pairwise key \( K_c \) to node \( u \) in a message encrypted and authenticated with pairwise key \( K_a,u \) between \( a \) and \( u \).

If the direct key establishment fails, the mobile sink and the sensor node will have to establish a pairwise key with the help of other sensor nodes. To establish a pairwise key with mobile sink \( v \), a sensor node \( u \) has to find a stationary access node \( a \) in its neighborhood such that node \( a \) can establish a pairwise key with both nodes \( u \) and \( v \). if node \( a \) establishes a pairwise key with only node \( v \) and not with \( u \). As the probability is high that the access node \( a \) can discover a common mobile polynomial with node \( v \), sensor node \( u \) needs to find an intermediate sensor node \( i \) along the path \( u--i--a--v \), such that intermediate node \( i \) can establish a direct pair wise key with node \( a \).

The use of mobile sinks in WSN introduces a new security challenge. wireless sensor network with one mobile sink and a base station. Sensor nodes store the generated data in their buffers. The mobile sink traverses the network using random walk, periodically transmitting beacon signals. Sensor nodes that hear the mobile sink’s beacon transmission begin transferring their aggregated data to the mobile sink. Since the mobile sink’s beacon signal received by sensor nodes is not authenticated, an adversary can attack the network by placing a malicious mobile sink.

The key exchange can be achieved by ECDSA (Elliptical Curve Digital Signature Algorithm).

ECDSA is an asymmetric key exchange algorithm. It allows exchanging a secret key though the network is vulnerable. It encrypts the symmetric key with a minimum energy cost.

### III. PROBLEM DESCRIPTION

#### ALGORITHM AND ANALYSIS

1. Formulas for calculation of polynomials:
   - Special case: \( \lambda = 1 \).
   - Each node has an id \( r_U \) which is unique and is a member of finite field \( Z_p \).
   - Three elements \( a, b, c \) are chosen from \( Z_p \).
   - Polynomial \( f(x,y) = (a + b(x + y) + cxy) \mod p \) is generated.
   - For each node polynomial share \( g_u(x) = (a_n + b_n x) \mod p \).

   \( \lambda \) example:

   - 3 nodes: U, V, W, with the following id’s 12, 7, 1 respectively
   - \( p=17 \) (chosen parameter)
   - \( a=8, b=7, c=2 \) (chosen parameters)
   - Polynomial \( f(x,y) = 8+7(x+y)+2xy \)
   - \( g \) polynomials are
     - \( g_u(x) = 7 + 14x \)
     - \( g_v(x) = 6 + 4x \)
     - \( g_w(x) = 15 + 9x \)
   - \( U \) computes \( K_{u,v} := g_u(r_v) = 7+14*7 \mod 17 = 3 \)
   - \( V \) computes \( K_{v,u} := g_v(r_u) = 6+4*12 \mod 17 = 3 \)

#### Dynamic Programming and Serialization

Dynamic Programming is a technique for solving problems with overlapping sub problems. Each sub-problem is solved only once and the result of each sub-problem is stored in a table (generally implemented as an array or a hash table) for future references. These sub-solutions may be used to obtain the original solution and the technique of storing the sub-problem solutions is known as memorization.

Serialization is the process of translating data structures or object state into a format that can be stored (for example, in a file or memory buffer, or transmitted across a network connection link) and "resurrected" later in the same or another computer environment.

![Fig.3 Data flow Diagram](image-url)
IV. RESULTS AND DISCUSSION

Wireless sensor network is simulated using ns-allinone-2.34. It is assumed that the network is not having pre-existing infrastructure. The network is simulated using 50 nodes which are placed randomly in 1000 x 1000 m$^2$ area (also the scenarios with 75, 100 nodes are considered for testing). The minimum and maximum speed is set to 0 and 20m/s respectively and pause time is set to 25sec. The No. 5.1 shows the Nam file.

Above figure shows the simulation of network of 50 nodes with their transmission range.
Mobile sink – yellow color and are moving
Sensor nodes - green color and static
Access point (stationary nodes) - Black color are static

The TCL script of the project will shows that the how the node is communication with each other, how the neighboring node identified with sending the route, and then after authentication node is to be communicated.

Below figure shows that TCL script of the project with 50 nodes.

Performance for the system is analyzed by the two parameter Connectivity and security.
Connectivity
Probability of mobile sink established the secure link with the sensor nodes from any access point with taking ratio of stationary node and neighbor nodes. (x-ratio of stationary nodes, y-probability). \( P_{\text{connect}} \)

![Graph](image)

The graph shows that when number no neighboring nodes increases, the probability also increases, were \( P_{\text{conn_c}} \) show the number of neighbors.

Security
Probability \( P_r \) when the separate polynomial and compare in the case with single polynomial pools with no of capture nodes. (x-axis - avg. no capture sensor node, y-axis probability), \( P_d \)

![Graph](image)

Graph shows that if average no of access nodes are more as compare to sensor nodes, then the probability of capturing the has key is more for the attacker.

Results for Comparing Single and Double Polynomial pool
Graph describe that if single polynomial pools is used then probability of connectivity is decreased as compare to double polynomial

Results After Adding Replicated Mobile Sink

In above graph comparison is shown with Single polynomial pool and Double polynomial pool with and without the replicated mobile sink. Graph shows that the attacker can connect with other nodes with more probability using single polynomial pool, but the probability is less for connection using double polynomial.
V. CONCLUSION

The Three-Tier security architecture overcomes the drawbacks of existing system and gives the better resilience against the attackers. As two separate pools are used for the purpose of authentication the attackers would not be able to capture the node information. Using two separate key pools and few stationary access nodes which carry polynomials from the mobile pool in the network, an attacker may fail to gather sensor data.

Larger the pool size, lower the probability of two pairs of nodes sharing the same key. The number of keys to be assigned to each sensor does not depend on the size of the WSN which improve the network connectivity.

Based on the two polynomial pool-based key predistribution scheme substantially improved network resilience to mobile sink replication attacks as compared to the single polynomial pool-based key predistribution approach. Also it is not increasing the communication overhead.

Analysis indicates that 10 percent of the sensor nodes in the network carry a polynomial from the mobile pool. The attacker would have to capture around 2 times more nodes as compared to the single polynomial pool approach, to become authenticated nodes.

REFERENCES