Security in WSN using Polynomial Pool Based Mechanism

Chanchal G.Agrawal, J. B. Kulkarni

Abstract*: *For efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensor mobile sinks (MSs) are necessary in many wireless sensor network (WSN) applications, However, in sensor networks for pair wise key establishment and authentication between sensor nodes and mobile sinks exiting key predistribution schemes are used, the work of mobile sinks for data collection elevates a new security challenge: in the basic probabilistic and q-composite key pre distribution schemes, an attacker can easily obtain a large number of keys by tracing a small fraction of nodes, and hence, by deploying a replicated mobile sink preloaded with some compromised keys gain the control of overall network.

A three-tier general framework describe that allow the use of any pair wise key pre distribution scheme as its basic component. This scheme requires two separate key pools, one for the mobile sink to access the network, and one for pair wise key establishment between the sensors. As compared to the polynomial pool-based scheme this security framework has higher network resilience to a mobile sink replication attack.

Index Terms*: *Wireless Sensor Network, Random Key Predistribution, Mobile Sink, Hash, Prime, Key Distribution Center.

I. INTRODUCTION

Recent advances in electronic technology 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.

In section 2, project pre requirements are to be given like history and exiting methods. Section3 contain Programmer's design like mathematical model is provided including functional, non functional requirements, Dynamic programming and Serialization and also data flow architecture, also Turing Machine.

In section 4, Result are to be discuss Lastly section 5 shows Conclusions and References.

II. RELATED WORK

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.

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

Manuscript received on July, 2013.

Chanchal G. Agrawal, Computer Engineering, Pune University / Sinhgad College of engineering e, India.

Prof. J. B. Kulkarni, Computer Engineering, Pune University/ Sinhgad college of engineering e, India.

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 pair wise 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.

There is a tradeoff to be made between security and vulnerability that has to be considered based on the sensor network size and application.

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 (in 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.

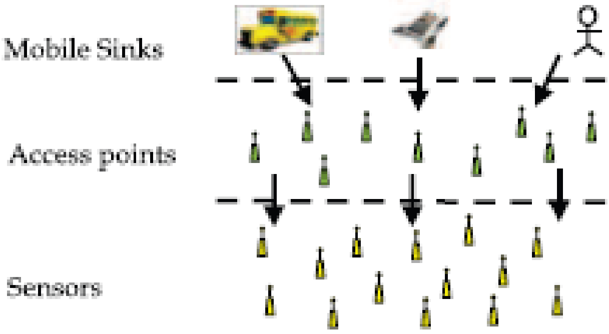


Fig 1. Three-Tier Security Architecture

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.

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.

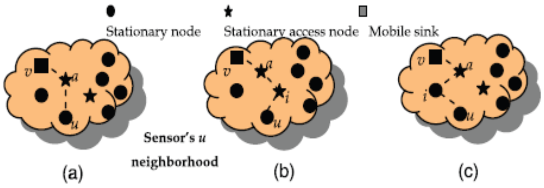


Fig 2. Node Description

This scheme is divided into two stages: static and mobile polynomial predistribution and key discovery between a mobile sink and a sensor node.

1. 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 Km and one polynomial (Km > 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 Ks and Ks -1 polynomials from S. Fig. 2 show the key discovery between the mobile node and stationary node.

2. 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 , EKv, v = 1, . . . ,|Ks_i|, where Kv is a potential pairwise key and the other node may have as suggests. When a direct secure path is established between nodes u and v, mobile sink v sends the pairwise key Kc to node a in a message encrypted and authenticated with the shared pairwise key Kv,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 Kc to node u in a message encrypted and authenticated with pairwise key Ka,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 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.

III. PROGRAM DESIGN

A. Mathematical Model

Let N be the proposed scheme: N = { r_u, Zp, P, F, λ a, b, c, , Gu(), a_n, b_n, K, u, v}Where,
λ = Collision resistance.
r_u = node id which is unique member of Zp.
Zp = Set keys that means polynomial pool.
a, b, c = Elements chosen from Zp.
P = Polynomial (some value).
F = Polynomial function.
Gu = Polynomial share.
a_n, b_n = factor used for calculation of Gu.
K = Key discovery function applied on particular node value.
u, v = node.
1. Zp = (Ru1, Ru2, Ru3,. . . ,Run) is the set of keys, {It is set of keys stored in pool }
2. u, v = Choosing node with unique id.
3. P = some value, and a, b, c= elements from Zp, Chosen parameter
4. F(x, y) =(a +b(x+y) + cxy) mod P, Finding value for polynomial.
5. Gu(x) =(a_n+ b_n) mod p, a_n=(a+br_u) mod P, b_n = (b+c r_u) mod P,Finding G polynomial.
6. Ku,v= Kv,u= f (r_u , r_v) = (a + b (r_u + r_v) + c r_u , r_v) mod p ,u computes Ku,v= Gu (r_v),v computes Kv,u= Gv (r_u) ,Computes key for communication between nodes

$$f(x,y)=\sum_{i=0}^{i=\lambda}\sum_{j=0}^{j=\lambda}a_{i,j}x^iy^j \bmod p;\ f(x,y)=f(y,x)$$

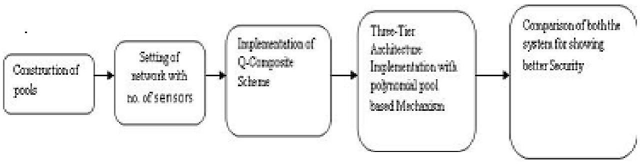
$$g_u(x)=f(x,r_u)\bmod p=\sum_{i=0}^{\lambda}a_{u,i}x^i$$

Polynomial based key pre-distribution scheme can be generalized to any λ by changing polynomials in the following way:
8. F(x, y), randomly generated, bivariate λ-degree, symmetric polynomial over finite field Zp, p ≥ n is prime.

B . 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.

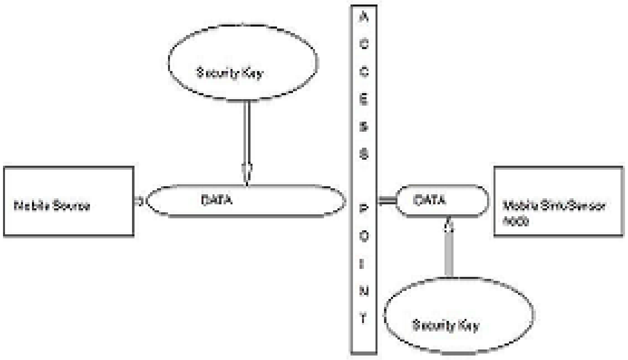
Serialization is the process of translating data structures or object state into a format that can be stored (for example, in a file or memory buffer, or transmitted across a network connection link) and "resurrected" later in the same or another computer environment.


Construction of pools
Setting of network with no. of sensors
Implementation of Q-Composite Scheme
Three-Tier Architecture Implementation with polynomial pool based Mechanism
Comparison of both the system for showing better Security

C. Data independence and Data Flow architecture

The ability to modify a scheme definition in one level without affecting a scheme definition in a higher level is called data independence. Physical data independence has ability to modify the physical scheme without causing application programs to be rewritten.

Modifications at this level are usually to improve performance. Logical data independence has ability to modify the conceptual scheme without causing application programs to be rewritten. It is usually done when logical structure of database is altered.

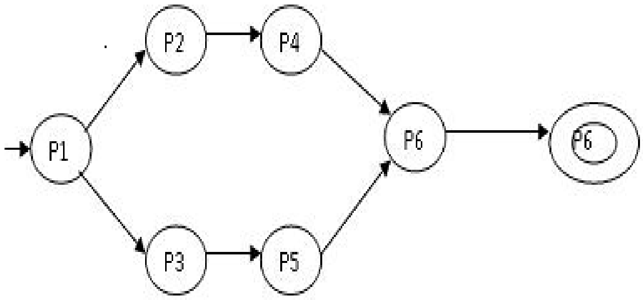


D. Multiplexer Logic

Multiprocessing systems include multiple complete processing units, multithreading aims to increase utilization of a single core by using thread-level as well as instruction-level parallelism. Techniques that would allow speedup of the overall system throughput of all tasks would be a meaningful performance gain.

E. Turing Machine

A Turing machine is a hypothetical device that manipulates symbols. Despite its simplicity, a Turing machine can be adapted to simulate the logic of any computer algorithm. A Turing machine can run forever, enter a loop, or reach a particular state or set of conditions.



Explanation of the related term of State diagram:
P1= Initial state setting of network.
P2= Distribution of keys to mobile sink form mobile polynomial pool and access nodes.
P3=Distribution of keys to sensor node form static polynomial pool and access nodes
P4= Making authentication between mobile sink and access point.
P5=Making authentication between access point and sensor node.
P6=Data transfer securely.
P7=Results.

IV. RESULTS ANG DISCUSSIONS

- The measure of the tolerance of the sensor network to node compromise.
- Number of keys or maximum network size. (x-no. of keys in key ring, y-estimated network size).
- 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).
- Probability of sensor node and a stationary node share a common static polynomial. (x- size of static polynomial pool, y-probability).
- Probability of two stationary node share common Static/mobile polynomial. (x-size of static polynomial, y-probability), (mobile polynomial pool size).
- No. of compromised nodes increases than what is the effect to the network. (x-no. of compromised nodes, y-probability(hash value compromised))

V. CONCLUSION

The Three-Tier security architecture will overcome the drawbacks of existing system and give the better resilience against the attackers. As two separate pools are used for the purpose of authentication the attackers would not able to capture the node information. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink.

Bigger the pool size is, the 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.

The proposed scheme, based on the polynomial pool-based key predistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach.

Further, the also improve the security performance of the proposed scheme against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes and sensor nodes.

REFERENCES

1. A. Rasheed and R.Mahapatra, "An efficient key Idstribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks", Proc.IEEE 27th Int'1 Performance Computing and Comm. Conf.(Ipccc '08),PP. 264-270, Dec.2008.
2. A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks", Proc. International Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC ’09), pp. 263-268,June 2009.
3. A. Rasheed and R. Mahapatra, "Three-Tier security scheme in wireless sensor network with mobile sink", IEEE Transaction on parallel and distributed system,vol-23,no.5,May-2012.
4. A. Rasheed and R. Mahapatra,"Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor network", IEEE Transaction on parallel and distributed system,vol-22,no.5,January 2011.
5. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung,"Perfectly-Secure Key Distribution for Dynamic Conferences", Proc. 12th Ann. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO ’92), pp. 471-486, 1993.
6. D. Liu, P. Ning, and R.Li. ,"Establishing Pairwise Keys in Distributed Sensor Networks", Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 52-61, Oct. 2003.
7. H. Chan, A. Perrig, and D. Song,"Random Key Pre-Distribution Schemes for Sensor Networks", Proc. IEEE Symp. Research in Security and Privacy, 2003.
8. H. Chan, A. Perrig, and D. Song,"Key Distribution Techniques for Sensor Networks", Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.
9. L. Eschenauer and V.D. Gligor,"Key-Management Scheme for Distributed Sensor Networks", Proc. ACM Conf. Computer Comm. Security (CCS ’02), pp. 41-47, 2002
10. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,,"Wireless Sensor Networks: A Survey", Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.
11. L. Lamport, “Password Authentication with Insecure Communication,” Comm. ACM, vol, 24, no. 22, pp. 770-772, Nov. 2982

AUTHOR PROFILE

Ms. Chanchal G. Agrawal completed BE in 2006 from Nagpur university .Now she is pursuing ME from the Pune university in Computer networks. She has five years of teaching experience.

Prof. J. B. Kulkarni working as a assistant professor in sinhgad college of engineering and completed ME form Pune university.