Detection Of Mobile Sink Replica In Wireless Sensor Network And Authenticate It With Key Distribution

Prameela. Bagewadi
Post Graduation Student [M.Tech II year]
The Oxford College of Engineering, Bangalore

Anil Kumar.K
Asst.Professor
The Oxford College of Engineering, Bangalore

ABSTRACT: **Authentication and pair wise key establishment are important where the security of mobile is concerned in the fast running wireless sensor network, where mobile sink is having more computational capability and , communication, energy supply, and storage capability. It acts as an agent to collect sensor readings. Therefore it is important to provide security to mobile sink against replication attack. In this paper, we are considering providing security to mobile sink against replication attack by means of exchange of keys between mobile sink and static sensor node. This security scheme allows the basic component as pair wise pre-key distribution over the network. In this scheme, two key pools are created one key pool for mobile sink authentication and other key pool is pair wise key establishment between the sensor nodes. To increase the efficiency of this scheme the authentication is provided between mobile sink and static sensor node which acts as a access point and between access points and dynamic sensor nodes.To increase the performance of the network, first the replica of the mobile sink is identified by means of observing the speed of the mobile sink in the network.**

Keywords: Security, Mobile sink, Authentication

I. Introduction

. Wireless Sensor Network have received a lot of attention due to their wide application in military as well as civilian and academic research field. These tiny sensors are randomly deployed in vital areas to sense the information or monitoring net[1]work area. Mobility has made faster communication , using mobile elements or mobile sinks . Mobile sink will collect all data from each sensor node, this sensed data often need to send to the base station for analysis purpose .Fig 1 shows the sensor network with mobile sink, which is used for data collection 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[2]. Therefore mobile sink or mobile elements are in need for faster transmission of the data. Security issues are considered on mobile elements, it should be protected from adversary attacks .WSN needs secure communication between the base station, sensor node and mobile sink from the adversary attacks. To make secure communication, authentication is provided between sensor nodes and mobile sink by exchanging the keys. The Sensor network attacks can be classified as Identity attack ,Routing attack and Intrusion Detection. Identity attacks intend to steal the identities of legitimate nodes operating in the sensor network. Node replication attack is identity attack ,where an adversary will add one or more nodes to the network that use the same ID as another node in the network. Reason for choosing this attack is that it can form the basis of a variety attacks such as Sybil attack, routing attacks and link layer attacks etc. also called as denial of service attacks which affects the availability of the network.

Fig 1.Sensor Network with Mobile sink

II. Related Work

Wireless nature of communication, lack of infrastructure and uncontrolled environment improve capabilities of adversaries in WSN. Stationary adversaries equipped with powerful computers and communication devices may access whole WSN from a remote location. Since sensor are randomly deployed in network, any adversaries can plant their own sensor nodes, base stations or cluster heads in uncontrolled environments. They can replace, compromise or physically damage existing ones.So security is very essential factor for sensor node and all mobile elements[2] .so some of security requirements for WSN are: *Availability*: ensuring that service offered by whole WSN, by any part of it, or by a single sensor node must be available whenever required, *Authentication*: authenticating other nodes, cluster heads, and base stations before granting a limited resource, or revealing information, *Integrity*: ensuring that message or the entity under consideration is not altered, *Confidentiality*: providing privacy of the wireless communication channels to prevent eavesdropping. *Key connectivity* (probability of key-share): probability that two or more sensor nodes store the same key or keying material. Enough key connectivity must be provided for a WSN to perform its intended function Key distribution is a central problem in cryptographic systems, and is a major component of the security subsystem of distributed systems, communication systems, and data networks[3]. Various key distribution schemes have been proposed so far, mainly to pairs of users (session keys). A basic and straightforward perfectly-secure scheme, which is useful in small systems consists of distributing initial keys to users in such a way that each potential group of users shares a common key.

Eschenauer and Gligor[4] first proposed a random key pre distribution scheme as before deployment, each sensor node receives a random subset of keys from a large key pool; to agree on a key for communication, two nodes find a common key, if any within their subsets and use that key as their shared secret key. Now, the existence of a shared key between a particular pair of nodes is not certain but is instead guaranteed only probabilistically this probability can be tuned by adjusting the parameters of the scheme. Eschenauer and Gligor note that this is not an insurmountable problem as long as any two nodes can securely communicate via a sequence of secure links. A generalization of this is the “q-composite” scheme which improves the resilience of the network (for the same amount of key storage) and requires an attacker to compromise many more nodes in order to compromise additional communication links. The difference between this scheme and the previous one is that the q-composite scheme requires two nodes to find q (with q > 1) keys in common before deriving a shared key and establishing a secure communication link. It is shown that, by increasing the value of q, network resilience against node capture is improved for certain ranges of other parameters.

Blom’s scheme uses a single key space to ensure that any pair of nodes can compute a shared key[5]. Motivated by the random key pre-distribution schemes described previously [Eschenauer and Gligor 2002; Chan et al. 2003], a new scheme using multiple key spaces. That is, we first construct ω spaces using Blom’s scheme, and then have each sensor node carry key information from τ (with $2 \le \tau < \omega$) randomly selected key spaces. Now (from the properties of the underlying Blom scheme), if two nodes carry key information from a common space they can compute a shared key.

Polynomial pool-based key pre distribution, which uses a polynomial pool instead of a key pool in [Eschenauer and Gligor 2002; Chan et al. 2003]. The secrets on each sensor node are generated from a subset of polynomials in the pool. If two sensor nodes have the secrets generated from the same polynomial, they can establish a pair wise key based on the polynomial-based key pre distribution scheme. An enhanced scheme using the t-degree bivariate key polynomial . They developed a general framework for pair wise key establishment using the polynomial-based key pre distribution protocol and the probabilistic key distribution . Their scheme could tolerate no more than t compromised nodes, where the value of t was limited by the memory available in the sensor nodes.

III Proposed Scheme

In the proposed scheme, the sensor network is divided into three layers which contains the mobile sinks which collects data from all sensor nodes, Second layer is static sensor nodes which acts as a access points between mobile sink and sensor nodes, these access points authenticate mobile sink and sensor nodes by exchanging the key, which in turn protects from adversary attacks on the network. The third layer is sensor nodes which are deployed in hostile environment to collect the information like temperature, events happening around the area[6]. this sensed data need to send to the base station for analysis so these mobile sinks are used for faster communication. With this scheme this paper identifies the replication attack on mobile sink and authenticate the same for secure communication.

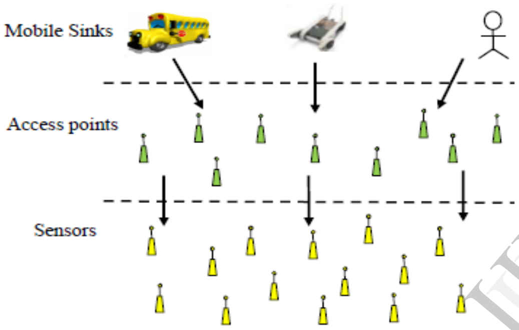

Fig 2.Three Layered wireless sensor network with mobile sink

A.Replication Attack Detection

Replication attack ,which is identity attack where the id of a node is copied by the attacker and create his own node with same which may lead to loss of data. This paper describes the replication attack on mobile sink which carries the critical information. Since mobile sink move around the network to collect the data from the sensor nodes. Mobility provides hint for solving problem of node replication attack detection that a mobile sensor node never move faster than the system maximum speed[8]. Therefore, if we examine that the mobile node speed is over the maximum speed, and then at least two nodes with the same identity are present in the network.

The base station computes the speed from every two consecutive claims of a mobile node and compares, by taking speed as an observed sample. Each time maximum speed is exceeded by the mobile node; it will expedite the random walk to hit or cross the upper limit and thus lead to the base station declares that the mobile node has been replicated. On the other hand, each time the maximum speed of the mobile node is not reached, it will expedite the random walk to hit or cross the lower limit and thus lead to the base station declares that mobile node has not been replicated.

B.Security Scheme for Mobile sink

First, for starting the replication attack, an adversary captures mobile sink deployed in the network where the adversary wants to obtain information for achieving adversarial goals. After that, the adversary makes replicates of mobile sink using the secret information or its ID extracted from the captured sinks and then deploys the replicates into the targeted areas. In the proposed security scheme ,a small fraction of the preselected sensor nodes called the static access nodes ,act as authentication access points to the network ,to trigger the sensor nodes to transmit their aggregated data to mobile sinks .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 .The attacker would also have to capture sensor nodes that carry 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 key generation is done using the RSA algorithm, which is known as public key algorithm.RSA algorithm is used for generation of Private and Public key, Which are distributed between mobile sink pool and static sensor pool.The keys are generated of key length 1024 bits to make secure communication,where the two prime numbers are splitted as 512 bits each.The RSA algorithm is choosen because of its cryptographic nature and to avoid the overhead in three layered network.

C Key Discovery between Mobile sink, Access points and Sensor nodes

To provide Secure communication between all the nodes ,this paper provides secure algorithm by creating the two separate polynomial pool as:*Mobile polynomial pool* and *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. Before the deployment process, each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool. The key discovery happen in three ways that is :*Direct key discovery, InDirect key discovery through intermediate stationary node i and InDirect stationary access node i*

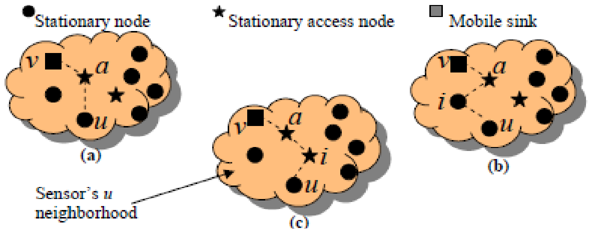

Fig.3Key Discovery(a) Direct key discovery, (b)InDirect key discovery through intermediate stationary node i and (c)InDirect stationary access node i.

These key generated are distributed between all the three layers randomly.The number of mobile polynomials in every mobile sink is more than the number of mobile polynomial in every stationary access node**.**The keys are assigned randomly as a subset of 40% of the keys from mobile sink to static access nodes and 80% to mobile sink from the mobile polynomial pool.

IV.Simulation Results

This security scheme provides the authentication between mobile sink and sensor nodes through access node,by exchanging the keys for this connectivity and security analysis are checked.Using two polynomial key pool security is provided.

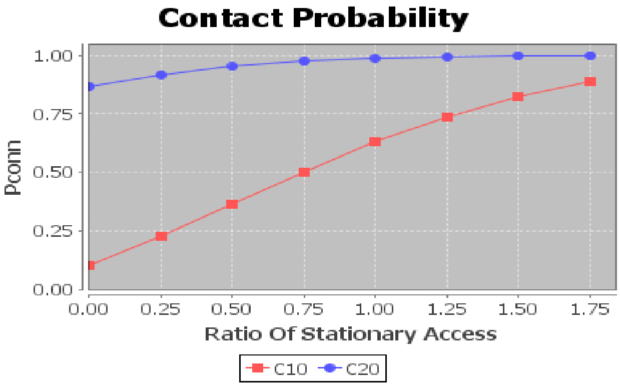

Fig 4.Probability of connectivity with stationary access nodes

From the graph, the connectivity is estimated as probability P_{conn} of a mobile sink establishing secure links with the sensor nodes from any authentication access point in the network as

$$Pconn = 1 - \left(1 - \left(\frac{c}{n}\right)^{m}\right)$$

Where **p** is the probability that a stationary access node and a sensor node share at least a common chosen password for access node verification **n** is total number of nodes**, c** is the average number of neighbor nodes for every sensor node before deployment of the stationary access nodes, and **m** is the number of stationary access nodes in the network.

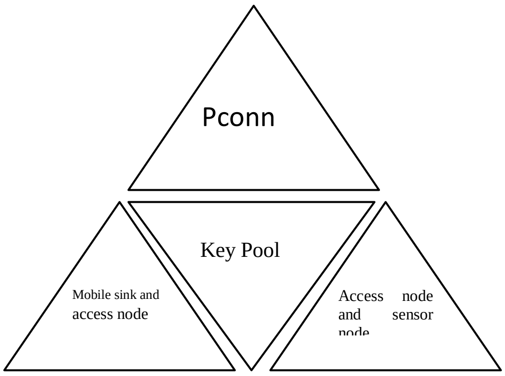

Fig 5.Key Pool between mobile sink,access nodes and sensor nodes

Fig 5 shows the key distribution between the two polynomials :Mobile polynomial pool and Static polynomial pool.By exchanging keys between them the security can be achived and connectivity can checked.

V. Conclusion

In proposed scheme, the three-layered wireless sensor network is created which help us in finding the replicates of the mobile sink in the network. By using the basic idea, that a mobile node never has velocity greater than the maximum velocity of system built up, the replication can be detected easily. For secure communication, two key pools are created as mobile polynomial pool and static polynomial pool by exchanging these keys authentication is provided between aii the three layers. By this we have achived security of mobile sink and connectivity between all the layers.

References

[1] 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.

[2] A. Becher, Z. Benenson, and M. Dornseif." Tampering with motes: Real-world physical attacks on wireless sensor networks". In *Proceedings of the 3rd InternationalConference on Security in Pervasive Computing (SPC)*,pages 104–118, 2006.

[3] A. Rasheed and R. Mahapatra, "An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks," Proc. IEEE 27th Int'l Performance Computing and Comm. Conf. (IPCCC '08), pp. 264-270, Dec. 2008.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proc. of the ACM Conference Computer Communication Security* (*CCS'02*), pp. 41-47, 2002

[5]R. Blom, "Non-public key distribution," In *Advances in Cryptology-CRYPTO'82,* D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. New York: Plenum Publishing, pp.
231-236, 1982.

[6] A. Rasheed and R. Mahapatra,"The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sink",Parallel and Distributed System,vol.23,no.5,May 2012.

[7] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," Proc. ACM MobiHoc, pp. 80-89,Sept. 2007

[8] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM*, pages 1917–1928, 2005

[9] Chia-Mu Yu, Chun-Shien Lu and Sy-Yen Kuo, "Efficient distributed and detection of node replication attacks in mobile sensor networks" IEEE 2009

[10] G. Ahmed, "Impact of Mobile Sink Speed on the Performance of Wireless Sensor Networks," vol. 1, no. 2, pp. 49–55, 2007.

[11] V. Manjula and C. Chellappan, "Replication Attack Mitigation for Static and Mobile WSN," vol. 3, no. 2, pp. 122–133, 2011.

[12] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks," Proc. Int'l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC '09), pp. 263-268, June 2009

[13] Nalini and Snehal ,"Mobile Node Replication Attack Detection in Wireless Sensor Network", International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1
ISSN 2250-3153

[14] H. Choi, S. Zhu, and T. F. L. Porta, "SET: Detecting node clones in sensor networks," in *Proc. Security Privacy Commun. Netw. Workshops*, 2007, pp. 341–350.

[15] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie,"Random-walk based approach to detect clone attacks in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 677–691, Jun. 2010.

[16] C. M. Yu, C. S. Lu, and S. Y. Kuo, "Mobile sensor network resilient against node replication attacks," in *Proc. IEEE Commun. Soc. Conf. Sensor Mesh Ad Hoc Commun. Netw.*, Jun. 2008, pp. 597–599.