ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (354-364), Month: April-June 2014, Available at: www.researchpublish.com

Security in Wireless Sensor Network using Stationary Access Nodes

[1]Sharath N, [2]Laxmi B Rananavare

[1]PG Student, [2]Associate Professor
Department of Computer Science and Engineering
Reva Institute of Technology and Management, Bangalore, India

***Abstract*: Wireless Sensor networks (WSNs) are easy to deploy and allow flexible installations which have enabled them to be used for numerous applications. Due to these properties, they face distinct information security threats. Security for WSNs is very much needed, because of its sensitive information transmission. Sensor networks are vulnerable to many types of attacks because they are deployed in public environment. So it is necessary to secure sensor networks, this can be achieved by introducing authentication and pair wise key establishment mechanisms to sensor nodes. In the proposed system some nodes in WSN are selected as stationary access nodes (SANs) to provide authentication access point between mobile sinks and static sensor nodes. The key distribution mechanism uses two types of key pools: the mobile key pool and the static key pool, the keys in the mobile key pool are shared between mobile sinks and SANs the keys in the static key pool are shared between Sans and Static sensor nodes.**

***Keywords*: Mobile sinks, Stationary access node, Pair-wise key distribution, Pre-distribution, Replication attack.**

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. Because of its easy to deploy and flexible installation features wireless sensor networks are used in wide range of applications such as, military sensing and tracking, health monitoring, data acquisition in hazardous environments, and habitat monitoring. Information flowing through WSN may be susceptible to eavesdropping, retransmit previous packets, injection of redundant bits in packets and many other threats of diverse nature. To ensure that the information being received and transmitted across these networks is secure and protected security schemes plays a vital role [1].

A typical sensor node contains transceiver, microcontroller, memory, power source, sensors and analog-to-digital converters. Sensor nodes are inexpensive, thus introducing many constraints in the performance parameters like storage capacity, power requirements and processing speed. The unreliable communication in WSN and unattended operation make the security defences even harder.

These sensors have the ability to communicate either among each other or directly to an external base-station (BS). A base-station may be a fixed node or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data. However, when the sensing field is too far from the base station, transmitting the data over long distances using multihop may weaken the security strength, therefore, mobile sinks (MSs) are essential components in the operation of many sensor network applications, including data collection in hazardous environments, localized reprogramming, oceanographic data collection, and military navigation. Wireless communication helps adversaries to perform variety of passive, active and stealth type of attacks. In passive mode, adversaries silently listen to radio channels to capture data, security credentials, or to collect enough information to derive the credentials. In active attacks, adversaries may actively intercept key management systems, capture and read the contents of sensor nodes. They can use wireless devices with various

capabilities to play man-in-the-middle or to hijack a session. They can insert, modify, replay or delete the traffic, jam a part or whole network. The security requirements of WSN are:

- Data Confidentiality
- Data Integrity
- Data Authentication
- Data Freshness
- Availability
- Self organization in WSN
- Secure Localization

Some common attacks an adversary can make to WSN are:

- Denial of Service (DoS)
- Collisions
- Exhaustion
- Unfairness
- Neglect and Greed attack
- Homing
- Routing Information Alteration
- Black holes
- Flooding
- De-Synchronization
- Interrogation
- Sybil Attack
- Selective Forwarding
- Worm holes Attack
- Hello Flood Attack
- Acknowledgement Spoofing
- Node Replication Attack

The countermeasures for some of the above mentioned attacks are specified in [1]. In this paper we are going to describe security services for WSN like authentication and pairwise key establishment with respect to node replication attack, by using a new security scheme called security in wireless sensor network using stationary access nodes (SANs).

.

II. RELATED WORK

A. Security Schemes and Key Management in WSN

To achieve security in WSNs, it is important to perform various cryptographic operations, including encryption, authentication, and so on. Selecting the appropriate cryptography method for sensor nodes is fundamental to providing security services in WSNs. However, the decision depends on the computation and communication capability of the sensor nodes. Since sensor nodes usually have severely constrained, asymmetric cryptography is often too expensive for many applications. Thus, a promising approach is to use more efficient symmetric cryptographic alternatives. However, symmetric cryptography is not as versatile as public key cryptographic techniques, which complicates the design of secure applications. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power, which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in WSNs. The security of a cryptographic system relies mainly

on the secrecy of the key it uses. Keys for these cryptographic operations must be set up by communicating nodes before they can exchange information securely. Key management schemes are mechanisms used to establish and distribute various kinds of cryptographic keys in the network, such as individual keys, pair wise keys, and group keys. If an attacker can find the key, the entire system is broken. In fact, a secure key management scheme is the prerequisite for the security of these primitives, and thus essential to achieving secure infrastructure in sensor networks. In Sensor networks end-to-end encryption is impractical because of large number of communicating nodes and each node is incapable of storing large number of encryption keys. Therefore hop-by-hop encryption mechanism is usually used in which each sensor node stores only encryption keys shared with its immediate neighbours.

TABLE I: Classification of Key Distribution

Keying Model	Approach	Mechanism	Keying Style
Pair-wise	Probabilistic	Predistribution	Random key-chain
			Pair-wise key
	Deterministic	Predistribution	Pair-wise key
			Combinatorial
		Dynamic key Generation	Master key
			Key matrix
			Polynomial
	Hybrid	Predistribution	Combinatorial
		Dynamic key Generation	Key matrix
			Polynomial
Group-wise	Deterministic	Dynamic key Generation	Polynomial

Some of the common keying models suitable for wireless sensor networks are pairwise keying and Group keying. These schemes further can be classified as shown in Table I.

There are two types of network model in WSN one is hierarchical WSN and other is distributed WSN, this survey paper deals with distributed WSN. In WSNs, sensor nodes use pre-distributed keys directly, or use keying materials to dynamically generate pair-wise and group-wise keys. Challenge is to find an efficient way of distributing keys and keying materials to sensor nodes prior to deployment. Solutions to key distribution problem in WSN can use one of the three approaches: (i) probabilistic, (ii) deterministic, or (iii) hybrid. In probabilistic solutions, key-chains are randomly selected from a key-pool and distributed to sensor nodes. In deterministic solutions, deterministic processes are used to design the key-pool and the key-chains to provide better key connectivity. Finally, hybrid solutions use probabilistic approaches on deterministic solutions to improve scalability and resilience.

Pair-wise key distribution schemes [5], [6], [9] are grouped according to proposed keying styles (i.e. pair-wise key, random keychain, master key . . .). Proposed schemes consist of three phases in general: (i) key setup prior to deployment, (ii) shared-key discovery after deployment, and (iii) path-key establishment if two sensor nodes do not share Straightforward approach is to use existing pair-wise keys to establish group-wise keys. For example, Lightweight key management system [Dutertre et al. 2004] considers a WSN where group of sensor nodes are deployed in different phases. It proposes to distribute group-wise keys through the links which are secured with pair-wise keys. Yet another

approach is to predistribute polynomial shares to sensor nodes by using which group members can generate a common group key. Polynomial based key pre-distribution scheme [Blundo et al. 1992] proposes two models. The first model is a noninteractive model where users compute a common key without any interaction. In the second interactive model, interaction is allowed in key computation.

B. Key Pre-Distribution Schemes

In key pre-distribution scheme the (secret) key information is distributed to all sensor nodes prior to deployment. Such schemes seem most appropriate for WSNs. If it is known which nodes will be in the same neighbourhood before deployment, pairwise keys can be established between these nodes (and only these nodes) *a priori* [2]. However, most sensor network deployments are random; thus, such *a priori* knowledge about the topology of the network does not exist. A number of key pre-distribution schemes do not rely on prior knowledge of the network topology. A naive solution is to let all nodes store an identical *master* secret key. Any pair of nodes can use this master secret key to securely establish a new pairwise key. However, this scheme does not exhibit desirable network resilience: if a single node is compromised, the security of the entire sensor network is compromised.

At the other extreme, one might consider a key pre-distribution scheme in which each sensor stores N - 1 keys, each of which is known to only one other sensor node (here, we let N denote the total number of nodes in the network). This scheme guarantees perfect resilience because any number of compromised nodes does not affect the security of any *un*compromised pairs of nodes. Unfortunately, this scheme is impractical for sensors with an extremely limited amount of memory because N could be large. Moreover, adding new nodes to a pre-existing sensor network is difficult when using this scheme because the existing nodes do not have the new nodes' keys.

Blom [Blom 1985] proposed a key pre-distribution scheme that allows *any* pair of nodes to find a secret pairwise key between them [3]. Compared to the "trivial" scheme mentioned earlier in which each node stores (N - 1) keys, Blom's scheme only requires nodes to store M + 1 keys, where $M << N$. The trade-off is that, unlike the (N -1)-pairwise key scheme, Blom's scheme is not perfectly resilient against node capture. Instead it has the following M-secure property: *as long as an adversary compromises at most M nodes, uncompromised nodes are perfectly secure. When an adversary compromises more than M nodes, all pairwise keys in the entire network are compromised.* The threshold M can be treated as a security parameter in that selection of a larger M leads to a more secure network. This threshold property of Blom's scheme is a desirable feature because an adversary needs to attack a significant fraction of the network in order to achieve high payoff. However, M also determines the amount of memory required to store key information, as increasing M leads to higher memory usage.

Recently, two key pre-distribution schemes suited for sensor networks have been proposed. Eschenauer and Gligor [Eschenauer and Gligor 2002] proposed a random key predistribution scheme which may be summarized as follows [8]: 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 with some probability (which can be tuned by adjusting the parameters of the scheme).

Based on this scheme, Chan, Perrig, and Song [Chan et al. 2003] proposed a generalized "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 any additional communication [4]. The difference between this scheme and the previous scheme 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 [Chan et al. 2003].

Blundo et al [6]. proposed several schemes allowing any group of n parties to compute a common key which is perfectly secret with respect to any coalition of t other parties [Blundo et al. 1993]. When n = 2, their main scheme may be viewed as a special case of Blom's scheme [Blom 1985].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (354-364), Month: April-June 2014, Available at: www.researchpublish.com

III. PROPOSED SYSTEM

In the proposed system a Wireless Sensor Network (WSN) consisting of *N* static sensor nodes and two mobile sinks (MSs) are created. Sensor nodes are independently and uniformly distributed over a planar surface. The network is homogeneous, in that all sensors are identical. Thus each node has the same amount of energy and uses the same communication range *R*. The mobile sink has a communication range *R*, and it traverses the network using a deterministic path with a speed *v*. In the N static sensors some nodes are selected as stationary access nodes (SANs), these SANs act as authentication access points to the WSN [12]. Fig 3.1 shows the architecture of the proposed scheme. In this system data gathered from sensor nodes are sent to the stationary access node. The SAN has selected by sensor nodes by two ways: *the SAN near to sensor nodes* and *the SAN paired by sensor nodes*, this scheme considers the later one.

A mobile sink sends data request messages to the sensor nodes via a SAN. These data request messages from the mobile sink will initiate the SAN to trigger sensor nodes, which transmit their data to the requested mobile sink. The scheme uses two separate key pools: *the mobile key pool* and *the static key pool*.

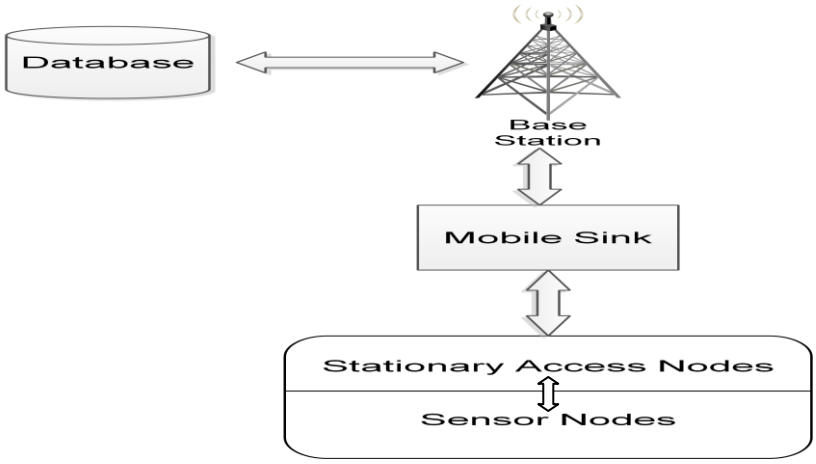

Fig. 1 Architecture of WSN with SANs

Using two separate key pools and having few SANs carrying keys from the mobile key pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink, this make it more difficult for an attacker to launch a mobile sink replication attack. The proposed system includes five modules they are described as follows:

A. WSN Creation:

In this module a network of N static sensor nodes, M SANs and P Mobile Sinks are created. The sensor nodes are deployed randomly in the network; the preselected SANs and mobile sinks are deployed in a particular position. Fig 3.2 shows the implementation of this module. The implementation is done using Matlab.

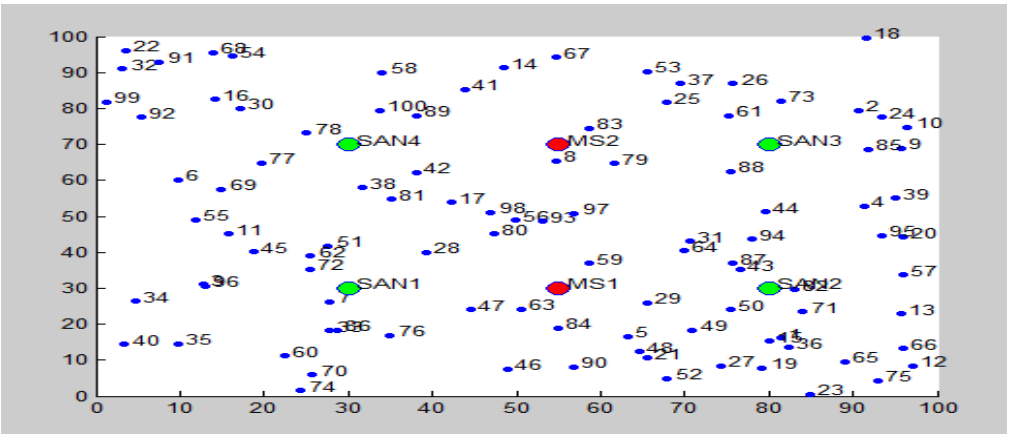

Fig. 2 WSN creation with static sensor nodes, SANs and mobile sinks

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (354-364), Month: April-June 2014, Available at: www.researchpublish.com

In this figure the blue colour circles indicates static sensor nodes, the green colour circles are SANs and the red colour circles are mobile sinks.

B. Mobile and Static Keys Distribution:

In this module the keys from the pre generated mobile key pool are shared between mobile sinks and SANs in such a way that the number of mobile keys in every mobile sinks is more than the number of mobile keys in every SANs (As shown in Fig 3.3). This guarantees that a mobile sink shares at least one common mobile key with SAN with high probability. Then the subset of keys from the pre generated static key pool are shared between SANs and Static sensor nodes (As shown in Fig 3.4).

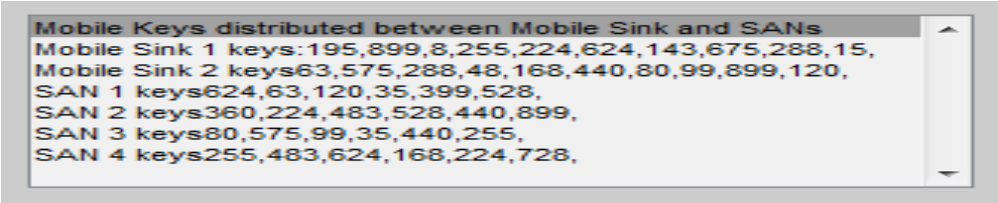

Fig. 3 Mobile keys distributed between Mobile sinks and SANs

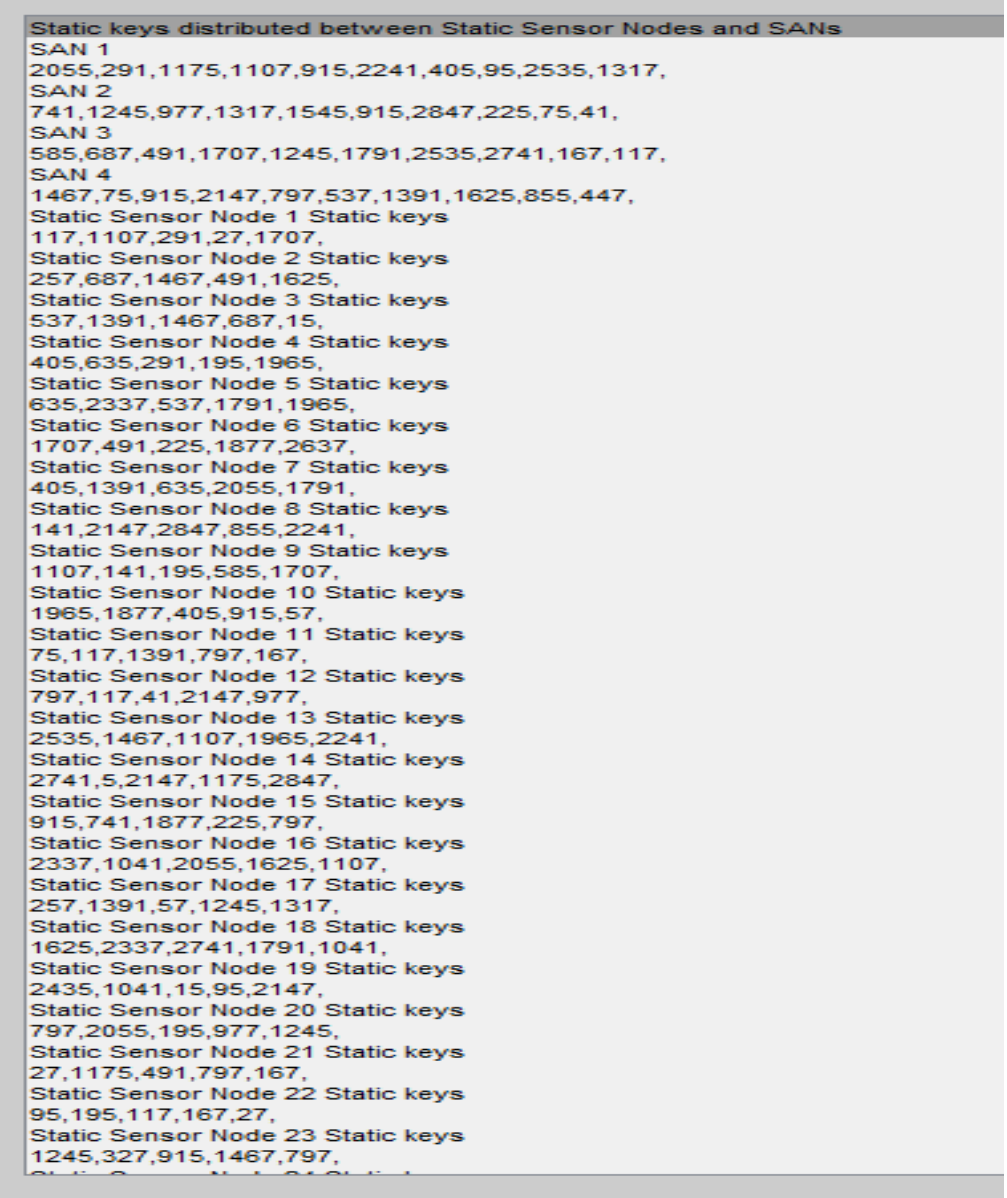

Fig. 4 Static keys distributed between Static sensor nodes and SANs

C. Pair Establishment:

The pairing between mobile sinks and SANs is done based on the mobile keys shared between them as described in previous module. For any mobile sink and SAN if there exist at least one common mobile key then they both can be paired. Same method applies for pairing between SAN and static sensor node, i.e. if there exist at least one common key from static key pool then they both can be paired (As shown in Fig 3.5).

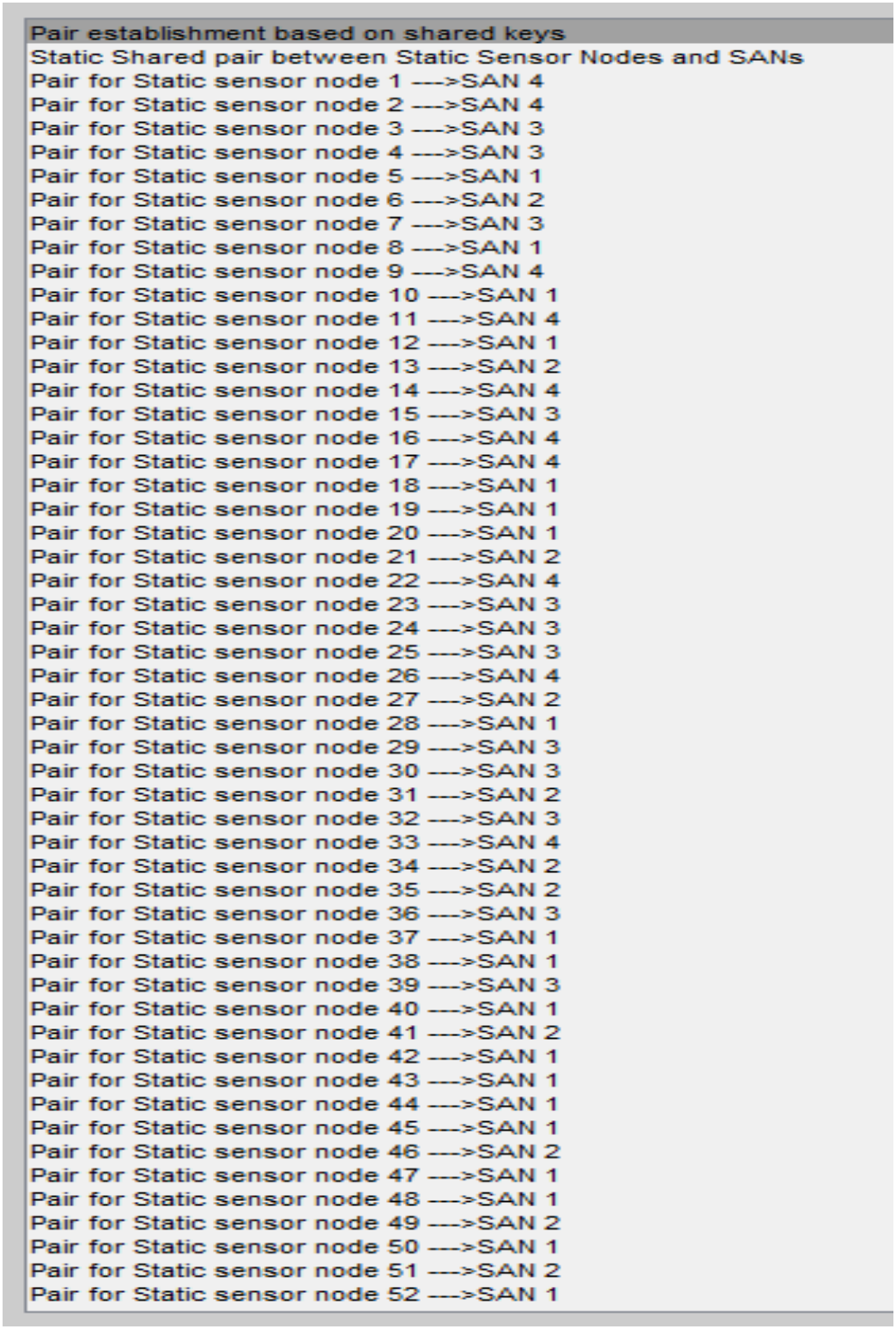

Fig. 5 Pair establishment based on shared keys

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (354-364), Month: April-June 2014, Available at: www.researchpublish.com

D. Password Distribution:

For each M SAN a different key is distributed and then all M keys are distributed to all static sensor nodes, this password distribution will be very useful in the case of SAN replication attack and that will be explained in latter section. The main purpose of the password distribution is authentication [10], [11].

E. Data Transmission:

In this module when the static sensor node have some data to send mobile sink, it will trigger SAN which it has paired, (in this example as shown in Fig 3.6 the sensor node 28 triggers SAN 1, the pairing for SAN 1 and sensor node 28 is shown in Fig 3.5) as it cannot sent data directly to the mobile sink, the sensor node send data to the SAN (indicated by dotted line from sensor node 28 to SAN 1and the data at SAN 1 is indicated by yellow colour at SAN 1). When the mobile sink traverse to the SAN, the data is given to the mobile sink by SAN (in this example when mobile sink 2 traverse to SAN 1 the data is taken by mobile sink 1, the colour of SAN return back to red, as shown in Fig 3.7).

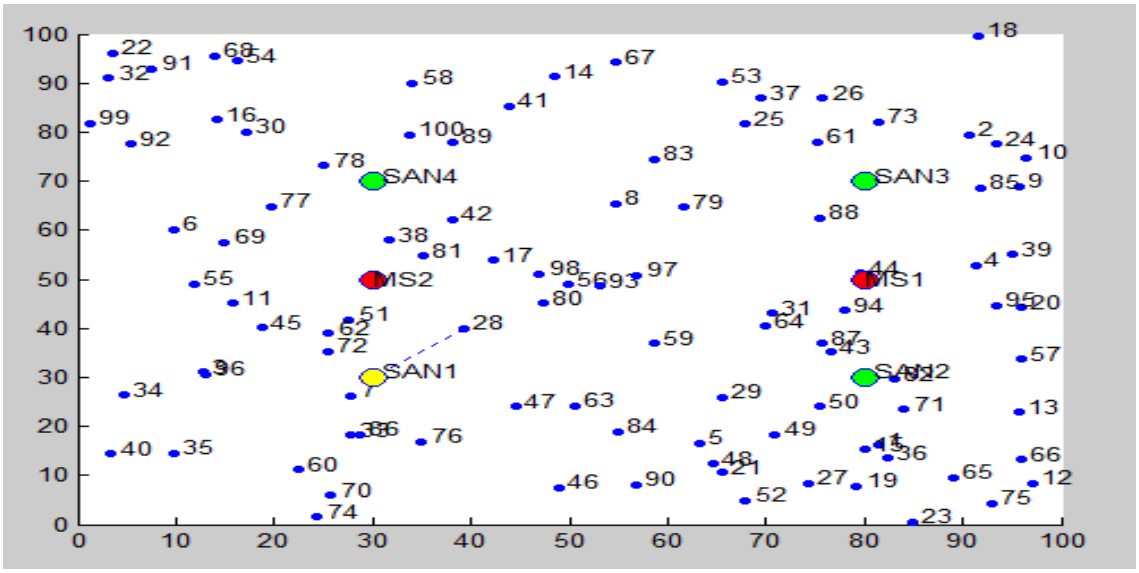

Fig. 6 Data transmission from Sensor Node to SAN

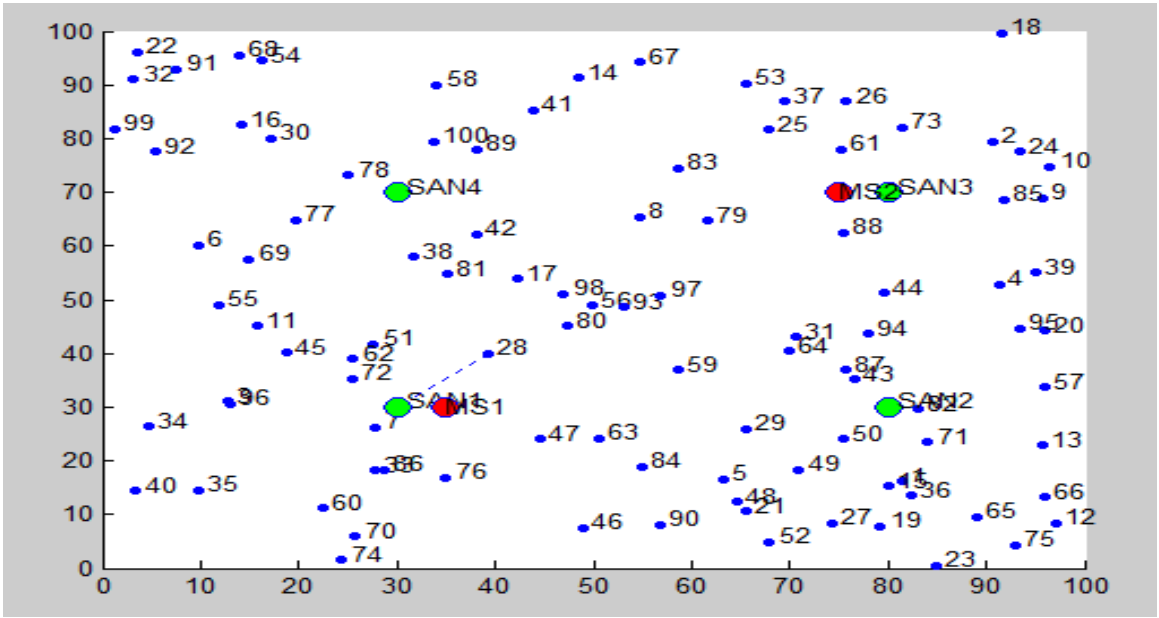

Fig. 7 Data transmission from SAN to Mobile Sink

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (354-364), Month: April-June 2014, Available at: www.researchpublish.com

IV. PERFORMANCE ANALYSIS

The performance of the proposed scheme can be analyzed using connectivity. In this the probability P_{Conn} equation 4.1 can be obtained which shows the probability of a mobile sink connecting securely with static sensor nodes from any SANs in the WSN.

$$P_{Conn} = 1 - (1 - c/n)^m \quad (4.1)$$

Where 'c' represents the average number of neighbor static sensor nodes for every static sensor nodes, m represents the number of SANs in the network. Fig 4.1 shows the probability of connectivity P_{conn} that a static sensor node has at least one SAN in its neighborhood versus the ratio of SANs (In Fig 4.1 the graph of four different values of c has been shown).

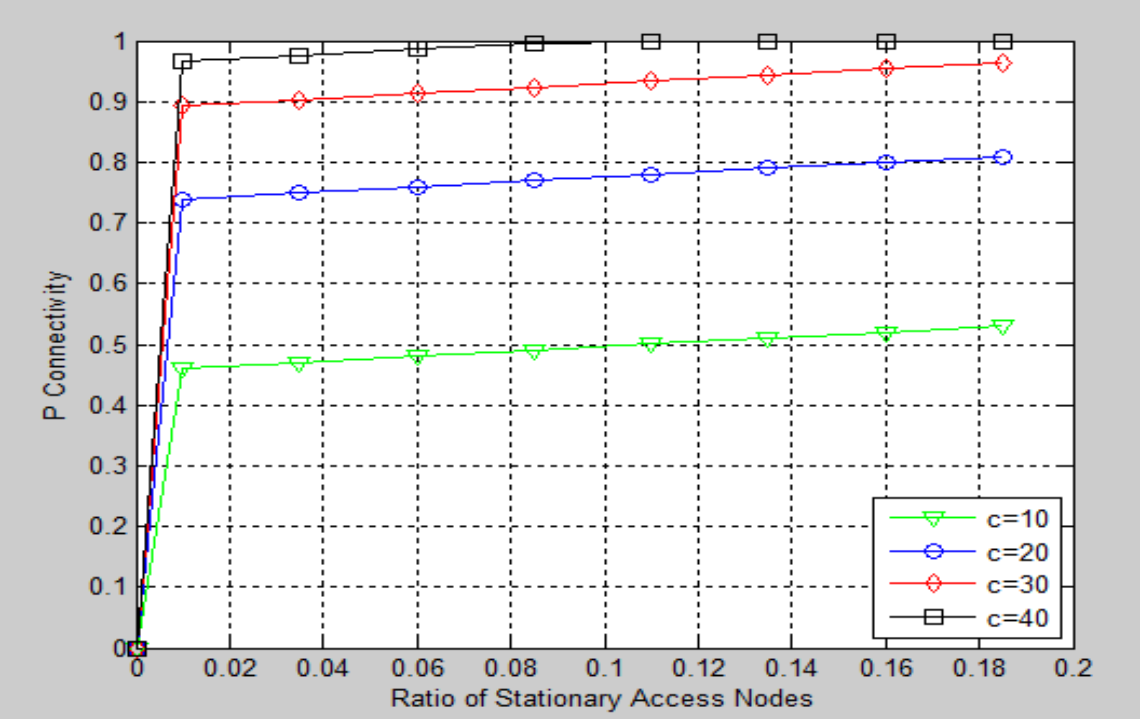

Fig. 8 Probability of connectivity versus the ratio of SANs in the network

V. THREAT ANALYSIS

In threat analysis the security performance of the proposed scheme is analysed against the *stationary access node replication attack* and *mobile sink replication attack*. An attacker to launch a mobile sink replication attack on the network, the adversary has to compromise at least one polynomial key from the mobile key pool. To achieve this, the adversary must capture at least a specific number of SANs that hold the same mobile polynomial. It follows from the security analysis of the *Blundo scheme*, that for any polynomial *w* in the mobile polynomial pool of degree t_m, an attacker cannot recover the polynomial *w*, if no more than t_m SANs that had chosen *w* are captured by the attacker. If more than t_m SANs with *w* as their mobile polynomial are captured by the attacker, then the attacker can recover the mobile polynomial *w*, and thus be able to launch a mobile sink replication attack against the sensor network. So care must be taken while distributing mobile keys to mobile sink and SANs, that no more than t_m SANs can share the same mobile key polynomial. Fig 5.1 shows the replicated mobile sink in the network, (indicated by pink colour circle showing MSR-1) when this replicated mobile sink introduced to the network, it fails to attack the network because it doesn't have enough number of mobile keys to pair with SANs.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (354-364), Month: April-June 2014, Available at: www.researchpublish.com

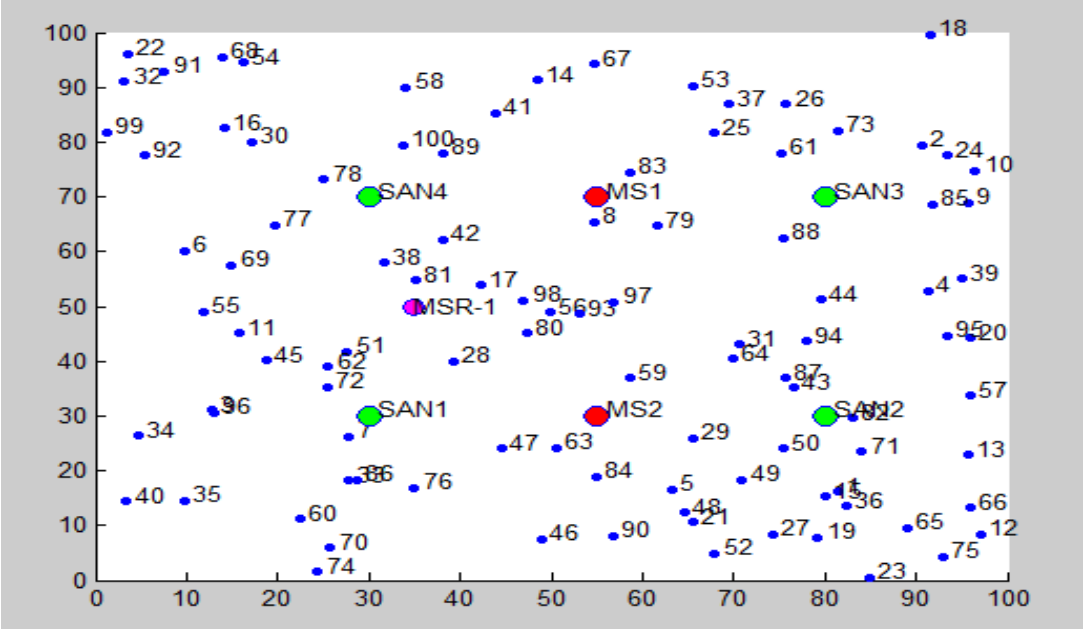

Fig. 9 Replicated Mobile Sink in the network failed to pair with SANs

In the case of a *stationary access node replication attack*, a one-way hash function is used in conjunction with the polynomial key pool scheme. In addition to the static keys, a pool of randomly generated passwords is used to enhance the authentication between static sensor nodes and SANs. To establish an authentication between a static sensor node and a SAN in the proposed scheme, the two must share a common static key. Also, they need to share a common hash function generated password. In the access node verification, to verify the authenticity of a SAN, the sensor node performs a single hash operation on the hash value that is sent from the SAN, this prevents the *stationary access nose replication attack*. Fig 5.2 shows the introduction of replicated SAN in the network (indicated by pink colour circle showing SANR-1).

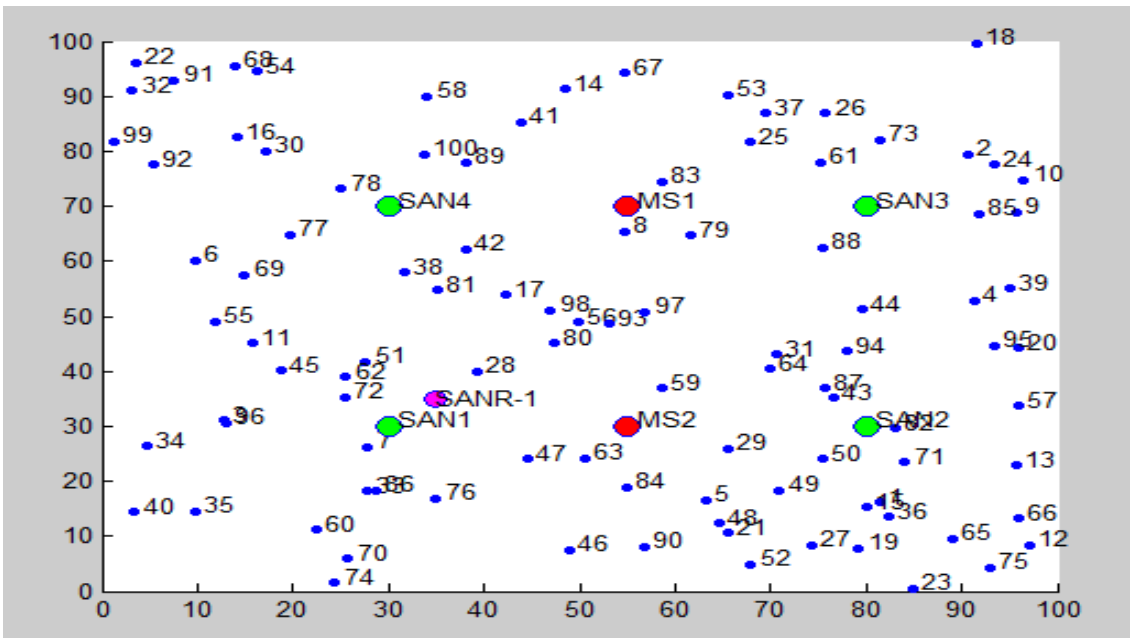

Fig. 10 Replicated SAN in the network failed to pair with static sensor nodes

VI. CONCLUSION

This security scheme for wireless sensor network using stationary access nodes improved the capability to overcome the two main attacks in the network, they are: *stationary access node replication attack* and *mobile sink replication attack.* The proposed scheme uses two key pools to provide security, they are: *static key pool* and *mobile key pool.* The *Stationary Access Nodes* carrying two separate key pools acts as authentication access point between static sensor nodes and mobile sinks. The main advantage of the proposed scheme is the SAN with keys from mobile key pool prevents mobile sink replication attack and the SAN with keys from static key pool and in conjunction with hash passwords prevents stationary access node replication attacks. If the adverse capture more than the specified polynomial degree of static sensor nodes than the probability of replication attack is high, this needs to be overcome in future. The performance of the proposed scheme is shown using probability connectivity graph.

REFERENCES

[1] M. Yasir Malik "An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations" *Institute of New Media and Communication Seoul National University, Korea*

[2] Du, Wenliang Kevin; Deng, Jing; Han, Yunghsiang S.; and Varshney, Pramod K., "A Pairwise Key Pre Distribution Scheme for Wireless Sensor Networks" (2000). *Electrical Engineering and Computer Science.* Paper 36.

[3] Blom, R. 1985. "An optimal class of symmetric key generation systems". *Advances in Cryptology: Proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, eds.), Lecture Notes in Computer Science, Springer-Verlag 209*, 335–338.

[4] Chan, H., Perrig, A., And Song, D. 2003. "Random key predistribution schemes for sensor networks". In *IEEE Symposium on Security and Privacy*. Berkeley, California, 197–213.

[5] Seyit A. Camtepe snd Bulent Yener "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey" Rensselaer Polytechnic Institute

[6] Blundo, C., Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., and Yung, M. 1992. "Perfectly-secure key distribution for dynamic conferences" In Crypto 92.

[7] Burmester, M. and Desmedt, Y. 1994. "A secure and efficient conference key distribution system" In Eurocrypt 94.

[8] Eschenauer, L. and Gligor, V. D. 2002. "A key-management scheme for distributed sensor networks" In 9th ACM conference on Computer and Communications Security.

[9] 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.

[10] 20 53 L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol, 24, no. 11, pp. 770-772, Nov. 1981.

[11] Perrig, A., Canetti, R., Tygar, J., and Song, D. X. 2000. "Efficient authentication and signing of multicast streams over lossy channels" In IEEE Symposium on Security and Privacy.

[12] A Rasheed and R N Mahapatra, **"**A The Three-Tier Security Scheme In Wireless Sensor Networks With Mobile Sinks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, NO. 5, May 2012