International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Node Clone Detection with Scalable Key Pre-Distribution Scheme for WSN

Rekha V. Aher[1], Sunita Nandagave[2]

[1]Student , Department of CSE, G. H. Raisoni College of Engineering, Pune, Maharashtra, India

[2]Professor, Department of CSE, G. H. Raisoni College of Engineering, Pune, Maharashtra, India

Abstract: ***The wireless sensor networks are characterized by resource constraint and large scalability. The wireless sensor networks are used in many critical application like military, health care services, industrial sectors etc. where highly secure transmission of data is required. An essential primitive in security which is a building block for any security service is pair wise key establishment. Wireless sensor networks are susceptible to the attack like node clone attacks, and there are several distributed protocols were proposed to detect this attack. However, the proposed protocols require much strong supposition to be practical for large-scale, randomly deployed sensor networks. In this paper, the system proposes two novel node clone detection protocols with great efficiency on network performance and condition. The first protocol is derived from a distributed hash table (DHT), by which a completely decentralized, key-based caching and checking system is constructed to catch cloned nodes effectively. The performance of protocol is improved with the help of probability model by efficient storage consumption and reducing the high security level theoretically. Then resulting equations with required adjustment for real time application are supported by simulations. Although the DHT-based protocol requires same communication cost as previous protocols, but for some scenario it may be considered as little high. To deal this, the randomly directed exploration protocol is emerged which provides better communication performance for large scale sensor network by probabilistic directed forwarding technique with random initial direction and border determination. The results of simulation preserve the protocol design and show satisfactory node clone detection probability and its efficiency on communication overhead. At the end we will compare this proposed system with those of existing methods for different criteria such as network scalability, storage overhead, network connectivity, network resiliency and average secure path length, and it is expected that this system will definitely improve the overall performance of the network as compared to existing ones.***

Keywords: Wireless sensor networks, Key pre-distribution, Key management, Network scalability, security.

1. Introduction

Nowadays the wireless sensor networks are attracted to use in various fields due to their efficiency and simplicity like hospitals, military services industry sectors etc.The sensor nodes are small battery powered devices with computing, data processing, and communicating components [1]. It is the great challenge to implement the security in wireless sensor networks because the resourse constraint on sensor node and network size. There are some securities schemes are available like public key cryptography which is widely used in network security. But in public key cryptographic method requires trusted third party to distribute the keys, also it needs more computational power and storage space, since sensor nodes are having limited storage space and computational capabilities. Therefore an alternative is only the symmetric key cryptography which ensures the secure communication and authentication between sensor nodes. In this method a pair wise key is established between sensor nodes. For this purpose the key is Pre-distributed among nodes before deploying the sensor nodes, so that called key-pre-distribution. There are various schemes are available for symmetric key management in WSNs namely probabilistic scheme and deterministic scheme. One of the major concerns while designing the key management scheme is network scalability. Therefore the approach should support the large number of nodes to enable large scale deployment of network. In the system, powerful assaulter can attack a limited number of authorized nodes and vitiate these nodes to get their confidential information, such as a pair of keys, credentials, and cryptograph information. With this secret information, a clone node can fraud intercommunicates with any of the nodes in the network and misleads it. Once replicas are added into the networks, adversary can get the incharge of entire network and different types of harmful attacks arise, including eavesdropping and modifying or replaying a message. Therefore there is a need to detect the node clone in the network as early as possible. Here this system is going to propose the two new protocol for node clone detection namely DHT and randomly directed exploration. The Distributed Hash Table is based on the hash value of the table that means key with the help of this key fully decentralised and key based checking and caching of system is established to catch node. The key plays very important role in DHT mechanism which determines the destination node of the message [6]. Another one is distributed detection protocol, called randomly directed exploration (RDE) in which probabilistic directed forwarding technique is embedded along with random initial direction and border determination is taken place. In this protocol every node contains signed version of neighbour list and the detection round is initiated by sending claiming message by the nodes to randomly selected neighbours.

2. Related Work: Key Management Schemes For WSNs

There is again one challenge while distributing the keys is key management. One way of distributing the keys among sensor nodes is a single common master key is distributed to all the nodes to secure sensor network which is efficient at optimal storage and better connectivity of network. But if that single key is compromised by adversary then the entire network will be insecure. Another way is to store the (N-1)

pair-wise keys to each sensor node for network size N. This approach overcomes the hazards of compromising a single key because adversary can't able to trace the keys since there are thousands of sensor nodes. But the storage requirement to store (N-1) keys is very high, where as the sensor nodes themselves are having very low storage and computational capability.

Therefore there are various types of symmetric key management scheme are available, mainly probabilistic scheme and deterministic scheme and those are again further divided. In deterministic scheme each two neighboring nodes can establish the direct secure link which ensures total secure connectivity with some probability. In probabilistic approach there is no guarantee of direct secure link since it requires existence of a shared key between two sensor nodes, if there is no direct secure link found between two nodes then they establish a secure path composed of successive secure link.

In last few years many pair wise key pre-distribution schemes are developed for wireless sensor network.

Probabilistic scheme-
1) Random key pre-distribution
2) Grid based scheme for group based WSNs
3) Random polynomial pre-distribution
4) Trade based key pre-distribution

Deterministic scheme-
1) SBIBD key pre-distribution
2) Master key based scheme
3) Third party based scheme

The first practical key pre-distribution scheme for sensor network was given by L. Eschenaur and Gligor [3].In this scheme a large key pool is generated before the deployment of sensor network, then each node fetches the block of keys from pool called key rings. Then each sensor node is having key ring with number of keys. After the deployment each node 'a' then shares it's list of key identifiers with its neighboring node 'b', so that node 'b' can able to find out the key that it shares with node 'a'. If two neighboring nodes shares at least one key, they establish a secure link and compute their session secret key which is common keys. This approach is energy and CPU efficient but it requires more memory to store the key rings. Hence further Chan et al proposed [2] extension to random key pre distribution called Q-composite scheme. In q-composite scheme two nodes should share q-keys to form a secure link. This approach good resilient against node capture since adversary needs to trace more than one key. In WSNs the key sharing is the crucial aspect so that in some of the existing work signal range of the sensor node is taken into consideration. Since it improves the key sharing mechanism. Huyen Thi & Mohsen Guizani [4] proposed the efficient signal range based key pre-distribution scheme for WSNs which included the probability key sharing of sensor nodes in same range is high than probability of key sharing of sensor nodes in different range. Camtepe and Yenar in [5] proposed the Combinatorial design for key pre distribution for WSNs. In this naive deterministic key pre distribution scheme is used based on Symmetric Balanced Incomplete Block Design (SBIBD) which allows to construct $m^2 + m = 1$ from key pool |S| such that each key ring contains $k = m + 1$ keys and each key ring shares exactly one common key . This campte scheme assures the greater secure connectivity. However SBIBD scheme does not scale to the very large networks.

3. Proposed Work

In proposed system, the aim is to take over the scalability issue without disgracing the other network performance metrics. For this purpose, the system focus on the the design of a scheme that ensures a better secure connectivity coverage for large scale networks with a good network resiliency and low key storage overhead. For this purpose, here the system uses the unital design theory for efficient WSN key pre-distribution. Also we are going to consider the signal range of each sensor node to effectively and efficiently calculate key sharing probability of the nodes. Since the sensor nodes are in same signal range having high probability of sharing common key than nodes in different signal range.

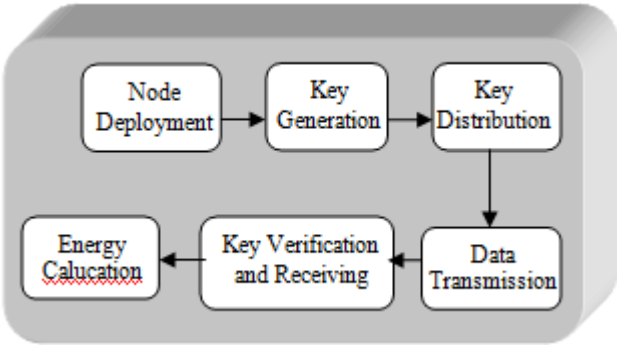

Figure 1: Block Diagram For Key Pre-Distribution

1. Node Deployment-

The first stage is Node deployment, where the numbers of nodes are deployed after key pre-distribution in the network. After specifying the number of nodes in the network, the nodes are deployed with unique ID (Identity) number and their energy level is also considered so that each can be differentiated.

2. Key Generation-
After the Node deployment, the key generation module is developed. The keys are generated by specifying number if blocks and number of nodes. The symmetric key is generated and is displayed in the text area given in the node.

3. Key Pre-distribution -
In this module, we generate blocks of n order initial design, where each block of key corresponds to key ring. Then pre-load each node with d completely disjoint blocks where d is a protocol parameter. In paper, system demonstrates the condition of existence of such d completely disjoint blocks among the unital blocks. Basically each node is pre-loaded with only one unital block and system proved that each pair of nodes share at most one key. Reverse to this, pre-loading each two nodes with d disjoint unital blocks means that each two nodes share between zero and keys since each two unitals blocks share at most one element. After the key distribution step, each two neighbors exchange their key

identifiers to determine the common keys. The proposed approach enhances the network resiliency since the adversary has to compromise more overlap keys to capture a secure link. Otherwise, if neighbors do not share any key, they must find a average secure path composed of successive secure links.

4. Secure Transmission with Energy

In this phase, the distance between two nodes is calculated and then nodes with their much neighbour information are displayed. Then the nodes which are much closer is selected and the energy level is first calculated to verify the secure transmission. After complete uploading the information, it is sent to the destination node. At receiver node, the key is compared and verified and then the data is received.

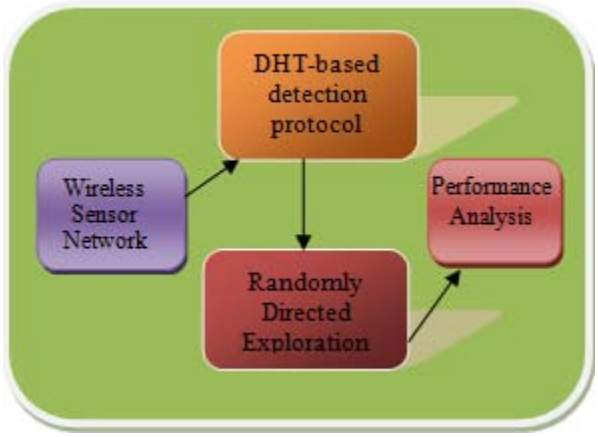

Figure 2: Proposed Block Diagram For System

Proposed system includes following:

- The naive mapping from unital design to key pre-distribution and system show through analytical analysis that it allows to achieve high scalability.
- For improving the good key sharing probability, the system proposed an enhanced unital based theory for good network scalability.
- This system will analyze and compare the new approach against those of existing schemes, with respect to different criteria: Energy consumption, network scalability, storage overhead, secure connectivity coverage, average secure path length and network resiliency.

4. Conclusion

This system proposes the new scalable key management scheme which ensures the secure connectivity coverage for large scale wireless sensor networks along with good network resiliency against attacker and low storage overhead. Here the system is going to use the unital design theory and then mapping from unitals to key pre-distribution ensures high network scalability, but this approach gives comparatively low key sharing ability. Hence enhanced unital theory is proposed which ensures high key sharing probability by maintaining unital theory results. This system is also going to conduct the analytical analysis of this new solution with existing ones with respect to the parameters like storage overhead, large network scalability, network resiliency, secure connectivity coverage, and average secure path length. The signal range assumption tends to the better improvement of the system. It is surely expected that this system will improve the overall network performance in wireless sensor networks.

References

[1] 'Securing wireless sensor networks –a survey' by Y. Zhou, Y. Fang, and Y. Zhang, *IEEE Commun. Surv. Tuts.*, vol. 10, no. 1–4, pp. 6–28, 2008.
[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *IEEE SP*, pp. 197–213, 2003.
[3] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 2002 ACM CCS*, pp. 41–47.
[4] Thi and Mohsen Guizan, An Efficient Signal-Range-Based Probabilistic Key Predistribution Scheme in a Wireless Sensor Network, *IEEE Transactions on vehicular technilogy*,vol.58,no.5,June 2009.
[5] S. A. Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 15, pp. 346–358, 2007.
[6] Zhijun Li, Member, IEEE, and Guang Gong,,".On the Node Clone Detection in Wireless Sensor Networks", in proc 5th IEEE transactions,Volume 40,no.11,pp 17-23,2013.