www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June , 2013 Page No. 2067-2071

SECURE COMBINATORIAL APPROACH IN WSN USING PAIRWISE AND TRIPLE KEY DISTRIBUTION

Mrs.Prathima.G, Mrs. Bharathi.M.A

Asst. Prof, Dept of Computer & Science & Engg. Global Academy of Technology Bangalore, India
E-Mail: prathima@gat.ac.in
Associate Professor, Dept of Computer & Science & Engg, RevaITM Bangalore, India
bmalakreddy@yahoo.com

Abstract— An addressing of the pair-wise and triple key establishment problems in wireless sensor networks (WSN) is been done. Several types of combinatorial designs have already been applied in key establishment. A *BIBD*(v, b, r, k, λ) (or $t-(v, b, r, k, \lambda)$ design) can be mapped to a sensor network, where v represents the size of the key pool, b represents the maximum number of nodes that the network can support, and k represents the size of the key chain. Any pair (or t-subset) of keys occurs together uniquely in exactly λ nodes; $\lambda = 2$ and $\lambda = 3$ are used to establish unique pair-wise or triple keys. Several known constructions of designs with $\lambda = 2$, to pre-distribute keys in sensors are used. A new construction of a design called *Strong Steiner Trade* and use it for pair-wise key establishment is described. To the best of our knowledge, this is the first paper on application of trades to key distribution. Our scheme is highly resilient against node capture attacks (achieved by key refreshing) and is applicable for mobile sensor networks (as key distribution is independent on the connectivity graph), while preserving low storage, computation and communication requirements. The introduction of a novel concept of triple key distribution, in which three nodes share common keys, and discuss its application in secure forwarding, detecting malicious nodes and key management in clustered sensor networks is made. Also presents a polynomial-based and a combinatorial approach (using trades) for triple key distribution. And also extend construction to simultaneously provide pair-wise and triple key distribution scheme, and apply it to secure data aggregation.

Keywords- Key pre-distribution, Pair-wise keys, Resilience, ***Secure-routing, Secure-aggregation, Steiner Trades***

I. INTRODUCTION

Sensor nodes are small battery powered devices which are deployed in large numbers to sense and collect information in various applications ranging from health care to military. In key pre-distribution, keys are preloaded in sensor nodes prior to deployment. A good key pre-distribution scheme should be *resilient* to node compromise. One way of pre-distribution is to load all the nodes with a single common master key, resulting in an optimal storage and full connectivity of the network. However, if one node is compromised then the entire network becomes insecure. At the other extreme, each pair of nodes can share a unique key (called pair-wise key). If there are N nodes in the network, then each node stores $N - 1$ pair-wise keys (*naive pair-wise scheme*). Such network has perfect resilience to node compromise, defined as follows: captured node reveals no information about links that it is not directly involved in, assuming captured node only reveals its own keys. However, the storage requirement for such a scheme can be very high. For a network consisting of 10,000 nodes the storage for the keys alone is about 160 Kilo Bytes (assuming keys are 128 bits long). Flash memory can be used in sensors; however, the storage for keys itself would be quite high, increasing the cost of each sensor considerably. Sensors devices have 10 Kilo Byte RAM and 48 Kilo Bytes of flash memory which is not sufficient for storing all the pair-wise keys. Perfect resilience is traded here for less storage requirements. Instead of deploying straight single pair-wise keys, which will be mostly idle in sparse and medium densities, pair of keys are needed, preserving space considerably. Another drawback is the time taken to access data from the flash memory. In applications where sensors need to establish pair-wise keys with several nodes, the access time increases greatly. This affects the overall performance. Sensor nodes are deployed after pre- distributing the keys. Depending upon the application, the deployment can either be random or arranged e.g. as square grid, triangular or hexagonal grids, in groups. Two nodes wishing to communicate securely must establish a common key.

Selected key distribution scheme should have the following desirable properties: 1) low memory cost, which is directly proportional to the number of keys stored, 2) high probability that two nodes within communication range are able to communicate securely using a common key, 3) low path length between two nodes that are within communication range; path may contain only links with endpoints sharing a common key, 4) high resilience to node compromise, and 5) low computation and commutation overheads to establish common key.

II. RELATED WORK

Haowen Chan et .al [1] has presented three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, they trade off the unlikeliest of a large-scale network attack in order to significantly strengthen random key redistribution's strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, they show how to strengthen the security between any two nodes by leveraging the security of other links.

Finally, they present the random-pair wise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation.

Wenliang Du et .al [2] has proposed a new key pre-distribution scheme, which substantially improves the resilience of the network compared to the existing schemes. Their scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold, the probability that any nodes other than these compromised nodes are affected is close to zero.

Mahalingam Ramkumar [3] has demonstrated a third approach where while the proxies aid the process of establishing pair wise secrets, the proxies are not trusted with the secrets of the sensors. They also presented two key redistribution schemes where the sensors can make effective use of the richer but entrusted resources of proxy devices to establish pair wise secrets. Consequently:-

1) The first no scalable scheme can realize "reasonably large" network sizes without the problem of susceptibility to collusions

2) The second scheme can support unlimited network size while achieving large collusion resistance

Claude Castelluccia and Angelo Spognardi [4] illustrated a new pre-distribution scheme adapted to multi-phase WSN. In the proposed scheme, the pre-distributed keys have limited lifetimes and are refreshed periodically. As a result, a network that is temporarily attacked (i.e. the attacker is active only during a limited amount of time) automatically self-heals, i.e. recovers its initial state when the attack stops.

Kishore Rajendiran et .al [5] has presented a novel approach to the above problem by making use of elliptic curve cryptography (ECC) is presented. In the proposed scheme, a seed key, which is a distinct point in an elliptic curve, is assigned to each sensor node prior to its deployment.

Neeraj Mittal et .al [6] has demonstrated a novel key redistribution scheme that makes use of region-based deployment knowledge. Their scheme constructs a set of clusters such that each cluster contains a small number of deployment regions, all of which are neighbors of each other. Furthermore, every pair of neighboring deployment regions belongs to at least one cluster. Each cluster has its own distinct key space, and it is from these cluster key spaces that nodes are assigned their keys. In this manner, they guarantee that nodes in neighboring regions share a key with a given overlap probability, while nodes in no neighboring regions do not share any keys.

Donggang Liu et .al [R7] has proposed two efficient instantiations of the general framework: a random subset assignment key redistribution scheme and a grid-based key redistribution scheme. The analysis in this paper indicates that these two schemes have a number of nice properties, including high probability (or guarantee) to establish pair wise keys, tolerance of node captures, and low communication overhead. Finally, this paper presents a technique to reduce the computation at sensors required by these schemes.

Richard Bean et .al [8] has focused on the representation of Steiner trades of volume less than or equal to nine and identify those for which the associated partial latin square can be decomposed into six disjoint latin interchanges.

Haowen Chan and Adrian Perrig [9] has presented fast and efficient primitives for broadcast authentication, public key management, and node-to-node signatures, each of which has important properties superior in some way to the current best known protocols in the literature. The reason for this performance is because they directly inherit, from the original secure data aggregation protocol, specific optimizations that work best in the structured tree network on which they operate.

Lingxuan Hu and David Evans [10] has present a protocol that provides a secure aggregation mechanism for wireless networks that is resilient to both intruder devices and single device key compromises. Our protocol is designed to work within the computation, memory and power consumption limits of inexpensive sensor devices, but takes advantage of the properties of wireless networking, as well as the power asymmetry between the devices and the base station.

Baruch Awerbuch et .al [11] has proposed an on-demand routing protocol for ad hoc wireless networks that provides resilience to byzantine failures caused by individual or colluding nodes. Their adaptive probing technique detects a malicious link after log n faults have occurred, where n is the length of the path. These links are then avoided by multiplicatively increasing their weights and by using an on-demand route discovery protocol that _nds a least weight path to the destination.

Deepak Ganesan et .al [12] has presented a novel braided multipath scheme, which results in several partially disjoint multipath schemes. They find that braided multipath is a viable alternative for energy-efficient recovery from isolated and patterned failures.

Hui Song et .al [13] has proposed two approaches to detect and accommodate the delay attacks. Their first approach uses the generalized extreme student zed deviate (GESD) algorithm to detect multiple outliers introduced by the compromised nodes; their second approach uses a threshold derived using a time transformation technique to filter out the outliers. Finally they

show the effectiveness of these two schemes through extensive simulations.

III. KEY DISTRIBUTION SCHEMES

The three simplest keying models that are used to compare the different relationships between the WSN security and operational requirements are: network keying, pair-wise keying, and group keying. The network keying model has inherent advantages over the other two schemes. It is simple, easy to manage, and uses very small amount of resources. Network keying also allows easy collaboration of nodes since neighboring nodes can read and interpret each other's data, satisfying the self-organization and accessibility requirements. It is also excellent in terms of scalability and flexibility because there is only one key for the entire network, and it does not change with the addition of nodes. However, an unacceptable drawback in robustness exists.

On the other hand, the pair-wise keying model employs N-1 keys in each node, assuming 'N' as the size of the network. Although this model provides the ultimate in robustness against node capture because the compromise of one node does not compromise any other node. It fails to satisfy the scalability requirement because the storage cost grows rapidly with network size.

The group keying scheme combines the features of both network and pair-wise keying schemes. Within a group of nodes that form a cluster, communications are performed using a single, shared key similar to network keying. However, communications between groups employ a different
key between each pair of groups in a manner identical to the pair-wise keying scheme. Thus, for a group of nodes, the accessibility requirement is satisfied because data aggregation can occur with no additional cost while some degree of robustness is maintained. When one of the nodes is compromised, the worst-case scenario is the compromise of the entire cluster that it belongs to, which is considerably more isolated than the entire network. In terms of scalability, an acceptable trade off is possible in this scheme, because the number of keys increases with the number of groups, not with the size of the network. However, the problem with this scheme is that it is difficult to set up and also, the formation of the groups is a very application dependent process. To efficiently distribute the keys, a keying scheme would require
group formation information.

IV. SECURITY MEASURES

Basic security measures include authentication, confidentiality, integrity, Non-Repudiation, Access control and privacy. However, in contrast to traditional wireless networks, physical security, of sensor nodes are not granted as they are usually deployed in remote and hostile environments. Therefore, attackers can easily compromise sensor nodes and use them to degrade the network's performance. Due to lack of physical security, the existing security solutions that are developed for traditional wireless networks cannot be directly employed. The security requirements of many protocols changed the situation and a more detailed research is currently underway to develop secure ad hoc routing protocols.

A. Authentication

Authentication is a major requirement as it ensures that the messages are sent by the actual nodes and hence attacks done by the greedy drivers or the other adversaries can be reduced to a greater extent. Authentication, however, raises privacy concerns, as a basic authentication scheme of attaching the identity of the sender with the message would allow tracking of vehicles. It, therefore, is absolutely essential to authenticate that a sending vehicle has a certain property which provides authentication as per the application.

B. Message Integrity

This is very much requires as this ensures the message will not change in transit that the messages the driver receives are not false.

C. Message Non-Repudiation

In this security based system a sender cannot deny the fact having sent the message. But that doesn't mean that everyone can identify the sender only specific authorities should be allowed to identify a vehicle from the authenticated messages it sends.

D. Entity authentication

It ensures that the sender who has generated the message is still inside the network and that the driver can be assured that the sender has send the message within a very short period.

E. Access control

It is required to ensure that all nodes function according to the roles and privileges authorized to them in the network. Towards access control, Authorization specifies what each node can do in the network and what messages can be generated by it.

F. Message confidentiality

It is a system which is required when certain nodes wants to communicate in private. But anybody cannot do that. This can only be done by the law enforcement authority vehicles to communicate with each other to convey private information. An example would be, to find the location of a criminal or a terrorist.

G. Privacy

This system is used to ensure that the information is not leaked to the unauthorized people who are not allowed to view the information Third parties should also not be able to track vehicle movements as it is a violation of personal privacy. However, in liability related cases, specified authorities should be able to trace user identities to determine responsibilities.

V. PROPOSED SYSTEM

The proposed system uses triple key that can be used in hierarchical sensor networks which typically consist of a base station (BS), cluster heads (CH) and sensor nodes. Each sensor is associated with a CH and sends sensed data to it. CH processes received data and forwards them to BS. If CH needs to monitor the communication between two nodes in its cluster then these three nodes need to share a unique common key. The prime aim of the proposed system is to design a secure framework using the concept of triple key distribution where the three nodes share the common keys for the purposed of secure data aggregation.

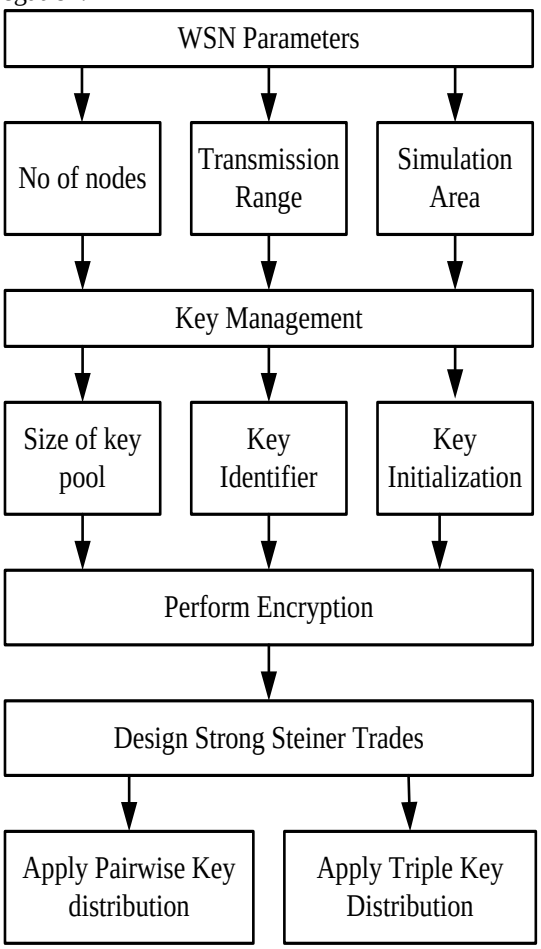

Figure 1 Schematic Diagram of Proposed System

The prime purposes of the proposed system are as following:

- To propose a new construction of Strong Steiner trades and describes their first application to key distribution in networks.
- To propose a new pair-wise key pre-distribution scheme using combinatorial structures for the purpose of highly resilient to node compromise and collusion attacks.
- To introduce a novel concept of triple key distribution in sensor networks in which every three nodes share a common key.
- To establish pairwise or triple key simultaneously among sensors.
- To apply triple key distribution to secure forwarding and key management in clustered sensor networks for secure data aggregation.

Diffie-Hellman protocol is a key agreement protocol between three parties. There is a one-round tripartite protocol, which is based on bilinear pairing is presented. A round consists of all the information that can be sent or received in parallel. Each node sends only one round of information about the keys it possesses and the members can calculate the common key in parallel, from these partial information. Joux's protocol is prone to man-in-the-middle attack. The sender/receiver will not recognize that it is sending the data to the intruder. To counter this, a proposal of an authenticated tripartite key agreement protocol is proposed. Tripartite key agreement has been a major topic of interest in cryptology. This relies on pairings on elliptic curve groups. Difficulty in choosing pairing friendly curves and expensive pairing operations make it difficult to be used in resource constrained sensor networks.

Also the several variations of the schemes are proposed. At initialization, each node is preloaded with a set of identifiers of nodes chosen at random. For each of these identifiers, a pair-wise key is also loaded in the node. After deployment, two nodes can communicate securely provided they have a pair-wise key. In a static network, nodes should be deployed so that they share pair-wise keys with their neighbors. However, in a dynamic network, new neighbors might not have pair-wise keys to communicate with each other.

Pair-wise schemes are preferred over other schemes because of increased security. In collusion attacks, an adversary might gather the information from many nodes to construct the pair-wise keys of the uncompromised nodes. Blom, Blundo and other schemes based on them are vulnerable to such attacks. In *c*-secure schemes, if an adversary compromises more than *c* nodes, then it can construct all the pair-wise keys of the uncompromised nodes.

In scenarios such as secure data aggregation and secure routing, an efficient session key needs to be established between two nodes. Pair-wise key distribution is a very effective and efficient way of establishing common key. Some of the schemes like PIKE establish pair-wise keys between nodes using the deployment position and are not suitable for mobile networks. Thus, attempt to design a scheme, which is secure against node compromise, can support mobile nodes, and has smaller or equal storage and communication overheads than existing schemes is taken into account.

VI. CONCLUSION

A design of new pair wise key establishment schemes in WSN using deterministic pre-distribution techniques based on

combinatorial designs is done. Combinatorial trades were applied for the first time for key pre-distribution in WSNs. And also present a new construction of strong Steiner trades. The schemes have advantage over other pair wise key schemes in terms of security and bandwidth requirements, and applicability to both static and mobile networks. An initiation of the study of triple key distribution in sensor networks, and applied it in secure routing, secure data aggregation and in communication in clustered sensor networks is carried out. Polynomial based scheme is applied so that every three nodes indeed have a common (and unique) key. This scheme is *c*-secure, where *c* is degree of polynomials used. An open problem is to design a secure routing algorithm using triple key, to preserve the anonymity and unlink ability of the network at the same time guaranteeing full security.

REFERENCES

[1] Haowen Chan, Adrian Perrig, "Dawn Song, Random Key Predistribution Schemes for Sensor Networks", Department of Electrical and Computer Engineering, 2003

[2] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney," A Pairwise Key Predistribution Scheme for Wireless Sensor Networks", ACM Transactions on Information and System Security (TISSEC) TISSEC Homepage archive , vol. 8, no. 2, pp.228-258, 2005

[3] Mahalingam Ramkumar," Proxy Aided Key Pre-distribution Schemes for Sensor Networks", Citeseer

[4] Claude Castelluccia, Angelo Spognardi, "RoK: A Robust Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks", CIteseer

[5] Kishore Rajendiran, Radha Sankararajan, and Ramasamy Palaniappan," A Secure Key Predistribution Scheme for WSN Using Elliptic Curve Cryptography" , ETRI, vol.33, no.5,2011

[6] Neeraj Mittal, Ramon Novales," Cluster-Based Key Predistribution Using Deployment Knowledge", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 7, NO. 3,, 2010

[7] Donggang Liu and Peng Ning," Establishing Pairwise Keys in Distributed Sensor Networks", CCS '03 Proceedings of the 10th ACM conference on Computer and communications security,pp. 52-61, 2003

[8] Richard Bean, Diane Donovan, Abdollah Khodkar, Anne Penfold Street, "Steiner trades that give rise to completely decomposable latin interchanges", Citeseer

[9] Haowen Chan and Adrian Perrig," Efficient Security Primitives Derived from a Secure Aggregation Algorithm", CCS '08 Proceedings of the 15th ACM conference on Computer and communications security, pp. 521-534

[10] Lingxuan Hu and David Evans, "Secure Aggregation for Wireless Networks", Citeseer

[11] Baruch Awerbuch, David Holmer, Cristina NitaRotaru and Herbert Rubens, "An OnDemand Secure Routing Protocol Resilient to Byzantine Failures", Citeseer

[12] Deepak Ganesan, Ramesh Govindan, Scott Shenker, Deborah Estrin," Highly-Resilient, Energy-Ef_cient Multipath Routing in Wireless Sensor Networks", Mobile Computing and Communications Review, Vol.1, no. 2, 2001

[13] Hui Song, Sencun Zhu, and Guohong Cao," Attack-Resilient Time Synchronization for Wireless Sensor Networks", Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference, pp.772, 2005