Vastly Efficient Key Pre Distribution and Authentication scheme for Wireless Sensor Networks

Eduru Hariprasad [#1], J.S.V.R.S.Sastry [*2,] N. Subhash Chandra[3]

[1]*pursuing M.Tech (IT), Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India*

[2]*working as Asst.Professor in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India*

[3]*working as Professor (CSE Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU-Hyderabad, A.P, India*

***Abstract*— The sensitivity of the potential applications of wireless sensor networks, security providing as a challenging issue in these networks. Due to the resource boundaries, symmetric key establishment is one favorite paradigm for securing WSN. One of the main concerns when designing a key authentication scheme for WSN is the network scalability. Indeed, the protocol should support a large number of nodes to enable a large scale deployment of the network. . Due to resource constraints, achieving such key agreement in wireless sensor networks is non-trivial. Many key authentication schemes used in general networks and public-key based schemes, are not suitable for wireless sensor networks. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. Recently, a random key pre-distribution scheme is proposed in that no deployment knowledge is available. We propose a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. So that the performance of sensor networks can be substantially improved with the use of our proposed scheme.**

***Keywords*— Wireless sensor networks, Key Authentication, Network Scalability, Resource Optimization.**

I. INTRODUCTION

Wireless sensor networks are growingly used in numerous fields such as medical, military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments and industrial applications they are mostly involved in several sensitive applications which require complex security services. In existing security systems due to the resource limitations for conventional networks could not be used in wireless sensor networks. So, the security issues became then one of the main challenges for the resource constrained environment of wireless sensor networks. Key Authentication is a corner stone service for many security services such as confidentiality and authentication which are required to secure communications in wireless sensor networks. The key establishment mechanism employed in a given sensor network should meet many requirements to be efficient. These requirements may include supporting in network processing and facilitating self-organization of data, among others. However, the key establishment technique for a secure application must minimally incorporate authenticity, confidentiality, integrity, scalability, and flexibility.

• **Authenticity:** The key establishment technique should guarantee that the communication nodes in the network have a way for verifying the authenticity of the other nodes involved in a communication, i.e., the receiver node should recognize the assigned ID of the sender node.

• **Confidentiality:** The key establishment technique should protect the disclosure of data from unauthorized parties. An adversary may try to attack a sensor network by acquiring the secret keys to obtain data. A better key technique controls the compromised nodes to keep data from being further revealed.

• **Integrity:** Integrity means no data falsification during transmissions. Here in terms of key establishment techniques, the meanings are explained as follows. Only the nodes in the network should have access to the keys and only an assigned base station should privilege to change the keys. This would effectively prevent unauthorized nodes from obtaining knowledge about the keys used and preclude updates from external sources.

• **Scalability:** Efficiency demands that sensor networks utilize a scalable key establishment technique to allow for the variations in size typical of such a network. Key establishment techniques employed should provide high-security features for small networks, but also maintain these characteristics when applied to larger ones.

• **Flexibility:** Key establishment techniques should be able to function well in any kind of environments and support dynamic deployment of nodes, i.e., a key establishment technique should be useful in multiple applications and allow for adding nodes at any time.

Symmetric key establishment is then one of the most suitable paradigms for securing exchanges in wireless sensor networks. Because of the lack of infrastructure in Wireless sensor networks, we have usually no trusted third party which can attribute Pair wise secret keys to neighboring nodes that is why most existing solutions are based on key pre-distribution. In this paper we propose an approach to enhance the scalability of wireless sensor network key management schemes without degrading significantly the other network performances and a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. We show that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can be substantially improved with the use of our proposed scheme.

II. RELATED WORK

Efficient Key Pre distribution and authentication problem in wireless sensor networks has been extensively studied in the literature and several solutions have been proposed. Many classifications of existing symmetric key management schemes can

be found. Here we describe several ways to provide security to keys that are used in wireless sensor networks throughout the communication between nodes in the network.

Key Management Scheme for Wireless Sensor Networks

Key management is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed. There are four principal concerns in a key management framework:

• How many keys are needed and how should the keys be distributed before the nodes are deployed? This is a problem of key deployment/pre-distribution.

• How does any pair of nodes or a group of nodes establish a secure session? This is a problem of key establishment.

• How should a node be added to the network such that it is able to establish secure sessions with existing nodes in the network, while not being able to decipher past traffic in the network (i.e. preserving backward secrecy)? This is a problem of member/node addition.

• How should a node be evicted from the network such that it will not again be able to establish secure sessions with any of the existing nodes in the network, and not able to decipher future traffic in the network (i.e. preserving forward secrecy)? This is a problem of member/node eviction.

The following discusses some of the most important work in the literature in terms of these four concerns.

I (i) Key deployment: A typical network-wide key deployment scheme where every node shares the same secret key called the group identity key.

(ii) Key establishment: All nodes in the network use the same traffic encryption key to communicate securely with each other. The traffic encryption key is derived as follows in two phases. In the first phase, the network starts with no clusters at all. Then every node broadcasts its weight and when a node finds its weight to be greater than its neighbors', it announces itself as the cluster head, while its neighbors become cluster members. The formation of the cluster is complete after the cluster head distributes a cluster key to its cluster members. The first phase ends with the cluster heads forming a backbone of the network. In the second phase, the cluster heads that have a larger weight than its neighboring cluster heads elect themselves as the potential key managers. After an exponential back off period, a potential key manager generates and distributes a traffic encryption key to other cluster heads. More than one potential key manager might generate a traffic encryption key at the same time, so a non- potential key manager's cluster head might receive more than one traffic encryption key. The cluster head chooses the traffic encryption key generated by the potential key managers with the largest weight, or the largest ID if the weights are equal.

II (i) Key deployment: Every node shares a unique master key with the base station. Compromising the base station thus compromises the communication in the entire network, although compromising a node only compromises the communication between the compromised node and the base station.

(ii) Key establishment: Two kinds of traffic are secured: node-to-node communications and broadcasts by the base station.

III (i) Key deployment: Every node is imprinted with k keys chosen at random from the key pool of size P.

(ii) Key establishment: Only node-to-node communications are supported. If the two nodes share at least a key, session keys are derived from the shared key(s). If the two nodes do not share any key, but have secure links to a common neighbor, then the two nodes can establish a session key through their common neighbor acting as a trusted third party. Note the two nodes in this context have to be within radio range; otherwise neighbor discovery cannot take place.

IV (i) for key deployment, they propose q-composite random predistribution, which is the same as original scheme, except in how the key pool size P is derived. As shown earlier, the expected degree (number of secure links) a node has is $p(n-1)$. If the number of expected neighbors within radio range is n', then the probability that a node is securely connected to any of its neighbors at all is $p(n-1)/n'$. Now P is calculated such that the probability the node shares at least q keys with any of its neighbors is greater or equal to $p(n-1)/n'$. As a consequence, every connection is now secured by a combination of at least q keys.

(ii) For key establishment, there are two options: (1) if the above q-composite scheme is used for key deployment, the session key is derived from an XOR of all shared keys; (2) if the basic scheme is used for key deployment, the session is derived using multipath key reinforcement. In multipath key reinforcement, two nodes that share Common neighbors can use their common neighbors to reinforce their secure links at the expense of communication efficiency.

III. CONSIDERATION METRICS FOR WSN

We consider mainly four metrics to compare performances of our solutions against existing ones:

I) Network scalability: represents the maximum number of generated key rings which corresponds to the maximum number of supported nodes. A large scale secure deployment of sensor networks relies strongly on this performance metric.

ii) Storage overhead: measures the memory required to store keys in each node. Because of their small size, sensor nodes are very constrained in term of memory resource and this metric is challenging. We focus, in this work, on the memory required to store keys and we omit the memory required to store the key identifiers when they are necessary. The key identifier size can be computed as the 2-logarithm of the maximum number of keys used by the protocol which is negligible compared to the key size.

iii) Probability of sharing a session key: computed as the probability that a given pair of neighboring nodes is able to establish a direct secure link through one or more common shared pre-deployed keys. This metric can also be seen as the fraction of secured direct links among possible links in the network.

iv) Average secure path length: when two neighboring nodes have no common keys, they should establish a secure path composed of successive secure links. This metric measures then the average length in hop count of these secure paths.

IV. RANDOM KEY PRE-DISTRIBUTION SCHEME

The major base scheme consisting of three layers in it. Key pre-distribution, shared-key discovery, and path-key establishment.

In the key pre-distribution phase, each sensor node randomly selects distinct cryptographic keys from a key pool, and stores them in its memory. This set of keys is called the node's key ring. The number of keys in the key pool is chosen.

After the nodes are deployed, a key-setup phase is performed. During this phase, each pair of neighboring nodes attempts to find a common key that they share. If such a key exists, the key is used to secure the communication link between these two nodes. After key-setup is complete, a connected graph of secure links is formed. Nodes can then set up path keys with their neighbors with whom they do not share keys. If the graph is connected, a path can always be found from a source node to any of its neighbors. The source node can then generate a path key and send it securely via the path to the target node.

The proposed algorithm a random block distribution allowing to pre-load t disjoint blocks in each sensor node.

Generate B =< Bq >, key sets corresponding to blocks of a unital design of order m

For each Node i **do**
KRi = {}
While (|KRi| ≤ t (m + 1)) **do**
Pick Bq from B
If ((KRi ∩ Bq) =Ø) **then**
KRi = KRi U Bq
B = B − Bq
End
End
End

Algorithm: A random approach of unital block pre Distribution in the enhanced unital-based scheme

V. PERFORMANCE EVOLUTION

To analyze the performance of our proposed scheme, we introduced the following parameters as a performance metrics.

1. Evolution Metrics

To represent desirable characteristics in a key-setup scheme for sensor networks we present the following criteria:

Connectivity:

We use global connectivity to refer to the ratio of the number of nodes in the largest isolated component in the final key-sharing graph to the size of the whole network. If the ratio equals 99%, it means that 99% of the sensor nodes are connected, and the rest 1% are unreachable from the largest isolated component. So, the global connectivity metric indicates the percentage of nodes that are wasted because of their unreachability. We use *local connectivity* to refer to the probability of any two neighboring nodes sharing at least one key. Both global connectivity and local connectivity are affected by the key pre-distribution scheme.

Communication overhead:

Since the probability that two neighboring nodes share a key is less than one, when the two neighboring nodes are not connected directly they need to find a route in the key-sharing graph to connect to each other. We need to determine the number of hops required on this route. Obviously, when the two neighbors are connected directly, the number of hops needed is 1. When more hops are needed to connect two neighboring nodes, the communication overhead of setting up the security association between them is higher.

2. System Configuration

In our analysis and simulations, we use the following setup:

- The size of the key pool = 100‹ 000.
- The number of sensor nodes in the sensor network is 10‹000.
- The deployment area is $1000m \times 1000m$.
- The area is divided into a grid of size 100 =10 × 10, with each grid cell of size $100m \times 100m$.
- The center of each grid cell is the deployment point.
- The wireless communication range for each node is R=40m.

3. Local Connectivity

We calculate the local connectivity as the probability of two neighboring nodes being able to find a common key. Let $B(n_i, n_j)$ be the event that node n_i and node n_j share at least one common key and $A(n_i, n_j)$ be the event that node n_i and node n_j are neighbors. Hence,

$$\text{Probability} = \Pr(B(n_i, n_j) \mid A(n_i, n_j)).$$

4. Global Connectivity

It is possible that the key-sharing in our scheme has a high local connectivity, but we have isolated components. Since those components are disconnected, no secure links can be established among them. Therefore, it is important to understand whether will have too many isolated components. We consider that all the nodes that are not connected to the largest isolated component are useless nodes because they are “unreachable” via secure links.

VI. CONCLUSION

We proposed, in this paper, Vastly Efficient Key Pre Distribution and Authentication scheme for Wireless Sensor Networks. We make use, for the first time, of the unital design theory. We showed that a basic mapping from unitals to key pre-distribution allows achieving extremely high network scalability while degrading the key sharing probability. We have described a random key pre-distribution scheme that uses deployment knowledge. With such knowledge, each node only needs to carry a fraction of the keys required by the other key pre-distribution schemes while achieving the same level of connectivity. The reduction in memory usage not only relieves the memory requirement on the memory constrained sensor node, but more importantly, it substantially improves network’s resilience against node capture. We have shown these improvements using our analytical and simulation results. Having demonstrated the dramatic improvement in the performance of the scheme, in our future work, we will investigate how much the deployment knowledge can improve the q-composite random key pre-distribution scheme and the pair wise key pre-distribution scheme. In addition, we will study the global connectivity, communication overhead, and the local resilience as we mentioned in the last section. Other deployment strategies and associated

distributions will also be considered.

REFERENCES

[1] Yun Zhou, Yuguang Fang, and Yanchao Zhang. Securing wireless sensor networks: A survey. IEEE Communications Surveys and Tutorials, 10(1-4):6–28, 2008.

[2] Wireless Integrated Network Sensors, University of California.

[3] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz. Comparing elliptic curve cryptography and rsa on 8-bit cpus. In CHES, pages 119–132, 2004.

[4] J. Zhang and V. Varadharajan. Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications, 33(2):63 – 75, 2010.

[5] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones. Security in wireless sensor networks. In Handbook of Information and Communication Security, pages 513–552. 2010.

Author Profile

Mr. Eduru Hariprasad currently pursuing M.Tech in the Department Of Information Technology, Holy Mary Institute of Engineering and Technology, JNTUniversity. His research interests include Network Security.

J.S.V.R.S.Sastry, Assistant Professor at Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD

Dr.N.Subhash Chandra, Professor (CSE Department) at Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD