A Novel Key Technique for Wireless Sensor Networks

Naeem Naik
ME in Computer Science, Vijayapura, India
E-mail: naeem.naik@gmail.com

Abstract: Key management is one in all the foremost vital issues of any secure communication. With the increasing demand for the transmission security in wireless detector networks (WSNs), it's pressing to introduce the secure and reliable key management scheme into the WSNs. during this paper, we have a tendency to projected a hierarchical key management theme to make sure the security of the network services and applications in WSNs. Scrutiny to the cluster key management protocol, our projected methodology will save a lot of computing and transmission energy through hierarchical style. Moreover, we improve the OFT (one-way hash perform tree) by CRT (Chinese Remainder Theorem) in order that it will be utilized in the large-scale WSNs. we have a tendency to designed some experiment to guage the protection and performance of this methodology, and also the experimental results show that the projected methodology are able to do satisfying results.

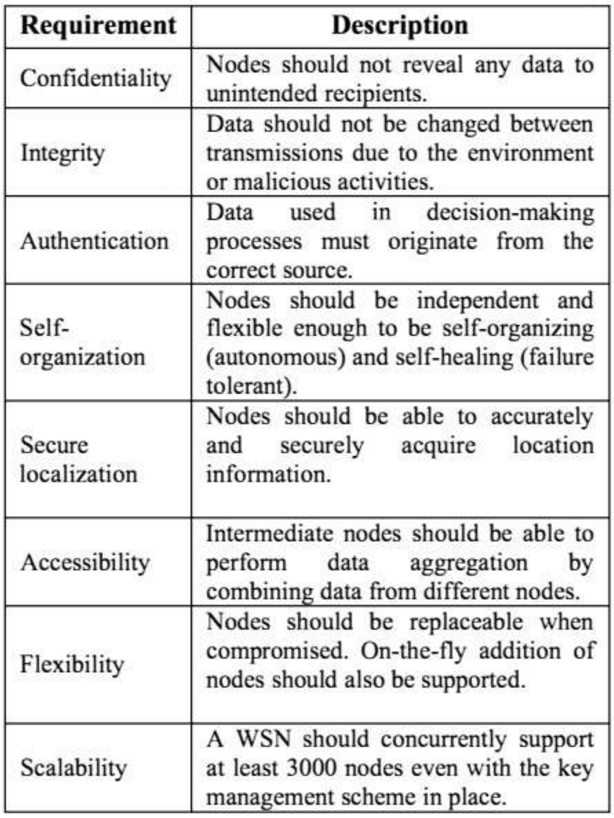
Keywords: Wireless sensor network; security protocol; key management

I. INTRODUCTION

The use of wireless sensors is on a pointy rise due to the very fact that they supply period of time watching and area unit probably low price solutions to a range of real-world challenges. However, once sensors are deployed in severe setting, especially, the adversary region, they're prone to be physically attacked. Thus, the protection of the network services and applications is one in every of the most serious issues forWSNs. Before a WSN will exchange knowledge firmly, encryption keys should be established among detector nodes. Key distribution refers to the distribution of multiple keys among the detector nodes, which is typical during a non-trivial security theme. Key managements could be a broader term for key distribution which also includes the processes of keys setup, the initial distributions of key and key revocations.

Table 1 shows the fundamental needs of WSNs. These needs act because the constraints within the design and realization of key management. During this paper, we have a tendency to propose a hierarchical key management theme to make sure the protection of the network services and applications in WSNs. The proposed technique will meet all the wants listed in Table one and it will save the computing and transmitting energy. Moreover, we have a tendency to improve the OFT[l] by CRT in order that it is employed in the large scale WSNs.

Table 1 Basic requirement for WSNs.



Requirement	Description
Confidentiality	Nodes should not reveal any data to unintended recipients.
Integrity	Data should not be changed between transmissions due to the environment or malicious activities.
Authentication	Data used in decision-making processes must originate from the correct source.
Self-organization	Nodes should be independent and flexible enough to be self-organizing (autonomous) and self-healing (failure tolerant).
Secure localization	Nodes should be able to accurately and securely acquire location information.
Accessibility	Intermediate nodes should be able to perform data aggregation by combining data from different nodes.
Flexibility	Nodes should be replaceable when compromised. On-the-fly addition of nodes should also be supported.
Scalability	A WSN should concurrently support at least 3000 nodes even with the key management scheme in place.

II. RELATED LITERATURE

Key management has remained a difficult issue in WSNs because of the constraints of sensing element node resources. Varied key management themes that trade off security and operational needs have been projected in recent years.

Eschenauer and Gligor[2] projected a straight forward and cost saving key management theme for theWSNs. Zhu and Steic[3] projected a hybrid key management scheme, LEAP, that uses a predistributed key to ascertain four styles of keys. However, since WSNs area unit dynamic networks whose topology area unit continually ever-changing, the above static key management schemes cannot meet the full demand of WSNs. Recently, researchers projected some dynamic key management schemes. Du[4] projected a robustness key management theme that provides node authentication in AN Eschenauer-like scheme. However, this technique does not support for cluster operation. Moreover, by victimization this technique, the nodes within the same watching space continually do the same job that result in high relative energy/time value. To support the cluster operation, some researchers introduce the cluster primarily based key management into WSNs, like RLKM[5], and so on. These cluster primarily based ways solve the problem of cluster operations successfully. To our greatest knowledge, the matter of the relative value has not been solved however.

In this paper, we have a tendency to propose a hierarchical key management theme that might save the relative cost scrutiny to the cluster primarily based ways.

III. Proposed Scheme

3.1 The topology of WSNs

As shown in Fig.l, the wireless detector networks used in this paper consists of head nodes (selected through some special formula, e.g., energy-based, location-based then on) settled at the middle of different watching space. In every watching space, there are variety of traditional detector nodes surrounding every head node and compose many groups, that is named terminal teams (TGs). In addition, we tend to build the subsequent assumptions regarding the configuration of the network.

1. All the detector nodes ar stationary.
2. Every detector node contains a buffer to avoid wasting the key information.
3. The detector nodes within the same TG discuss the communication key by some key agreements.
4. The key for various BGs ar freelance.
5. The detector nodes communicate with the top node by single-hop mode. the top nodes communicate with the sink node directly.

3.2 Logical structure of the system

To reduce the relative value within the key change process, we tend to propose a superimposed design cluster key management theme.

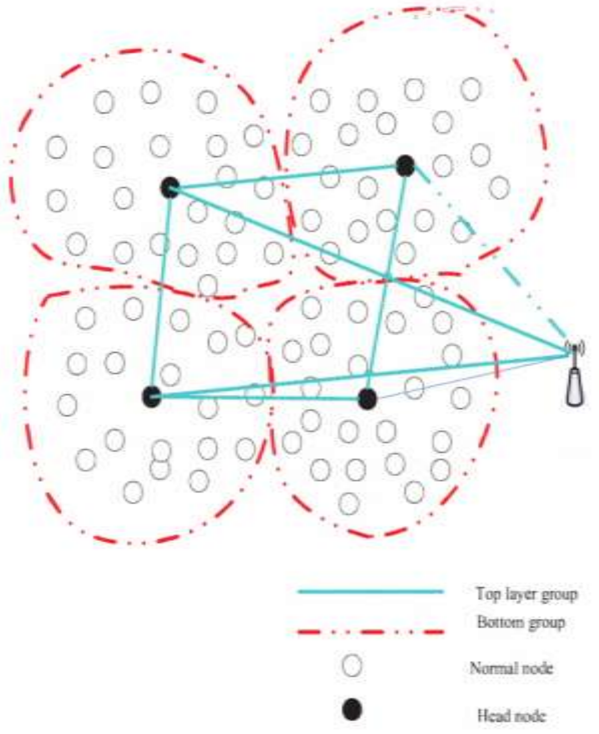


Figure 1. The architecture of the wireless sensor network

The projected system has 2 logical layers: the gateway layer and also the terminal layer.

- Master-node layer
  - Created of the top nodes;
  - Collect the node data of its motoring space and request the intergroup key from the sink;
  - Distribute the inter-group key to the terminal layer.
- Terminal layer
  - Created of the traditional nodes;
  - Request the communication key from the entry layer through causation identifcation data.

3.3 Protocol description

There are 2 crucial principles for the protocol design:

- Massive scale - the protocol are often applied to the WSNs, that have a varied sensing element nodes.

- Dynamic key management the communication keys are often update once a node be a part of or leave.
- Low redundancy value - totally different nodes (special the neighbor nodes) needn't to deal with the reduplicate messages.

To solve on top of issues, we have a tendency to adopt a unique key management protocol supported the structure described in Section 3.2. Within the planned protocol, the nodes {in totally different in several in numerous} layers use different ways to negotiate the communication keys. The methods for the entrance layer relies on OFT[I], while that of the terminal layer relies on CRT.

3.4 System deployment and initialization

According to cathode-ray tube, the sink generate a seed key pool: P={m,m2,m3, …,md} the seed keys are pairwise coprime and k is massive than N(the range of deployed node).

- Before deploying the sensing element nodes in hostile feld, the sink assign the seed key m; , secret key Xi and range IDlO every node.
- The nodes were deployed as Fig.I. Then many neighboring nodes kind a terminal group as Fig.I and generate a head node in accordance to election mechanism.

IV. Performance evaluation

4.1 Security analysis

The security of our theme is often explicit as follows:

- Forward secrecy

In wireless sensing element network, the node is extremely easy captured. Once a node was compromised and evicted, the cluster key should be update and the compromised node cannot cipher the future cluster key. In our theme, if a noral node leaves, the terminal cluster can establish a new cluster key consistent with cathode-ray tube. The compromised node cannot cipher the new group key. And if a head node was evicted, the 2 layer cluster can update two new cluster key, and {also the} evicted node also cannot cipher new key.

- Backward secrecy

When a replacement node be a part of the wireless sensing element network, rock bottom cluster that the node joined can update new cluster key. According to CRT, the new node cannot compromise any earlier key.

4.2 Performance analysis

Assumed that there ar N nodes in WSN, and d denotes the peak of the key tree. within the tree-based group key management theme [5], when a new node joins the WSN, the theme desires renew all the nodes, and therefore the communication quality is O(dlog-$_d$-d). once a node leaves the WSN, the communication quality is O(dlog$_d$). In our theme, once a node joins, the communication quality is O(B) , where B denotes the quantity of the terminal cluster nodes. When a node leaves, the communication complexity is as follows:

$$\begin{cases} O(B) & \text{a normal node leave} \\ O(\log_2^{\frac{N}{B}} + B) & \text{a head node leave} \end{cases}$$

Likelihood of the departure node is the same, and therefore the average of communication complexity is

$$O(\frac{1}{B} * (\log_2^{\frac{N}{B}} + B) + B - 1)$$

Above all, our theme reduces the burden of updating the cluster key once a node joins or leaves the WSN.

V. Conclusions

In this paper, we have a tendency to propose a class-conscious key management theme to confirm the safety of the network services and applications in WSNs.

Comparing to the cluster key management protocol, our planned methodology will save additional computing and transmission energy through class-conscious design. Moreover, we have a tendency to improve the OFT (one-way hash fnction tree) by CRT(Chinese Remainder Theorem) in order that it are often employed in the large-scale WSNs. we have a tendency to compare our theme to some wide used key management methodology through some experiment, and therefore the results show that the planned method can do satisting results.

References

1. Sherman, A.T.; McGrew, D.A.; , "Key establishment in large dynamic groups using one-way fnction trees," Software Engineering, IEEE Transactions on , vo1.29, no.5, pp. 444- 458, May 2003.
2. L. Eschenauer, V.D. Gligor. A keymanagement scheme for distributed MSN networks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS),
3. Washington DC, November 2002, pp. 41-7. [3] S. Zhu, S. Setia, and S. Jajodia, "LEAP Efcient Security Mechanisms for LargeScale Distributed Sensor Net-works," Proc. 10th ACM Conf Compo and Commun. Sec., 2003, pp. 62-72
4. W. Du, J. Deng, Y.S. Han, S. Chen, P.K. Varshney, A key management scheme for wireless sensor networks using deployment knowledge, in: Proceedings of IEEE INFOCOM'04, March 2004.
5. Li Lin, Wang Ru-chuan,Jiang Bo, Huang Hai-ping. Research of Layer-Cluster Key Management Scheme

on Wireless Sensor Networks [J]. Joural of Electronics & Information Technology, Vo1.28No.12 , 2006,pages: 2394-2397.