Comparative study on dynamic key-management techniques for cluster-based sensor networks

[1]Jaydeepsinh Barad, [2]Bintu Kadhiwala
[1]PG Student, [2]Asst. Prof.
[1]Department of Computer Engineering,
[1]SCET college, Surat, India
[1]baradjaydeepm@gmail.com, [2]bintu.kadhiwala@scet.ac.in

***Abstract*— Wireless sensor networks consist of sensor nodes with limited amount of resources and deployed in hostile or remote environment and unattended by human, they are prone to different kind of attacks. So security is a major concern in WSN and communication between nodes must be secure that important data do not compromised. For the same adaptation of dynamic key is very important for secure key management while encrypting data. Many techniques has been proposed regarding dynamic key management but because of the limitations of WSN like limited memory, battery life and processing power, increases the use of cluster-based wireless sensor network which reduces system end-to-end delay and energy consumption. In this work we have carried of the comparative study of different dynamic key management schemes based on cluster-based sensor networks and finally summarized on the bases of different evaluation metrics with pros and cons of each scheme.**

***Keywords*— Wireless sensor networks, Security, Key management.**

I. Introduction

Due to the wide range of application, wireless sensor networks (WSNs) have gained so much attention in few years. The network is built using sensor nodes which are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors [13]. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to the user [13].

Sensor nodes are the devices with low power and consist of one or more sensors, a processor, memory, a power supply, and a radio. A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure properties of the environment [6]. As nodes have limited resources and are generally deployed in locations which are unattended by human, so communication of the data are carried out using radio. Battery is the main power source in a sensor node [6]. As sensor nodes are deployed in hostile or remote environment and unattended by human, they are prone to different kind of attacks. WSNs are applicable in some of the sensitive areas like defense, battle field surveillance, target tracking. So data must be sent to a base station in a secure way using encryption techniques. So adaptation of key management is very important for WSNs. Key management is a core mechanism to ensure security in network and one of the major applications of wireless sensor network and can be defined as a set of processes and mechanism that support key establishment and the maintenance of ongoing keying relationships between valid parties according to a security policy [6]. The key management in WSNs consist of different process of creating, distributing and maintaining the secrete keys. So to generate techniques for key management for encryption, which can make data communication more secure and at a same time make less resource utilization, have vital importance in WSNs.

1.1 Related work and contribution

In WSNs, few good quality papers have been presented on key management but scope of the survey paper still differ from existing works in different aspects. We have gone through various surveys but no review paper is available where recent key management schemes for clustered based sensor networks are discussed thoroughly. As clustered based sensor network has many advantages, survey based on this architecture for dynamic key management becomes necessary. The goal of this study is to provide detailed view of key management for clustered based sensor network and to identify research direction for future work.

The remaining paper is organized as follow: Section 2 presents related work and evaluation metrics. Section 3 describes different schemes of key management. Section 4 consists of comparison of different technique and finally we and the work with conclusion.

II. Related work and Evaluation metrics

Due to various applications, the key management systems for WSNs have received increasing attention, and numerous key management schemes have been proposed for WSNs. Depending on the ability to update the cryptographic keys of sensor nodes during their run time (rekeying), these schemes can be classified into two different categories: static and dynamic[6].

In static key management, key pre-distribution scheme is used, and keys remain fixed for the whole lifetime of the network. However, in this case due to the same key, the probability of being attacked increases significantly. Instead, in dynamic key management, the keys are changed throughout the lifetime of the network. So Dynamic key management is very important type of key management in sensor networks. Dynamic key management is a set of processes used to perform rekeying either periodically or on demand as needed by the network. Since the keys of compromised nodes are revoked in the rekeying process, dynamic key management schemes enhance network survivability and network resilience dramatically [6].

In general, key management can be classified according to different criteria one of them is using the central key controller involved for new key generation and distribution. Generally the key management schemes can be classified as distributed or centralized. Distributed dynamic key management is a set of process, in which no central key controller, such as a base station or third party, is involved in rekeying process of sensor nodes [6]. Basic idea behind distributed dynamic key management scheme is to avoid a single point of failure by managing key using multiple key controllers. But these schemes are prone to design errors as compromised sensor nodes can participate in node eviction process. Whereas, centralized dynamic key management is a set of mechanisms that that uses a single central key controller, such as a base station or third party, to manage and replace key materials on the network's nodes [6]. Compared with distributed dynamic key management, it is impossible for compromised sensor nodes to damage the node eviction process in centralized key management scheme. It is further divided into flat, hierarchical and heterogeneous network based key management.

2.1 Evaluation Metrics

Dynamic key management can be considered as a branch of key management. All key management schemes should fulfil the following traditional security requirements: confidentiality, authentication, freshness, integrity and non-repudiation. The same holds for dynamic key management schemes.

The other merits of key management schemes are security, efficiency and flexibility [7] on the bases of what we have reviewed different papers.

1. Security Metrics

Dynamic key management schemes must provide the cryptographic keys in a secure manner, thwarting the activities of malicious nodes inside a network. Upon detecting a compromised sensor node, the current secret key of the compromised sensor node must be revoked and a new one must be generated and distributed to its associated sensor nodes, except the compromised one. Moreover, it is desirable for a dynamic key management scheme to maintain not only forward and backward secrecy, but also collusion resistance between the newly joined nodes and the compromised ones. In addition, resilience against node capture and node replication needs to be provided.

2. Efficiency Metrics

The number of message transmissions for rekeying, the required number of the cryptographic keys and the amount of operations must be kept as low as possible, meanwhile, the size of the cryptographic keys should be as short as possible. This prevents the network size from being bounded by the available energy resources and storage capacities of each node. The dynamic key distribution itself shall not put a heavy burden on the inherent resource constrained sensor nodes in terms of memory, bandwidth and energy.

3. Flexibility Metrics

Key establishment techniques should be flexible enough to function well in the wide range of scenarios covered by WSN applications. The most important flexibility metrics are mobility, scalability and key connectivity.

III. DYNAMIC KEY MANAGEMENT SCHEMES FOR CLUSTER-BASED WSNS

In this section, we discuss the major dynamic key management schemes proposed to date for clustered-based WSNs, and highlight the security and performance analysis of each scheme. Fig 1 shows the classification of different schemes which we have evaluated based on evaluation metrics. Almost all the schemes can be classified as asymmetric or symmetric key, based on the key used for encryption and decryption of message at sender and receiver side. If same key is used by both the party then it is known as symmetric key and if not then it is known as asymmetric key. Based on that we have evaluated different schemes which are as follow:

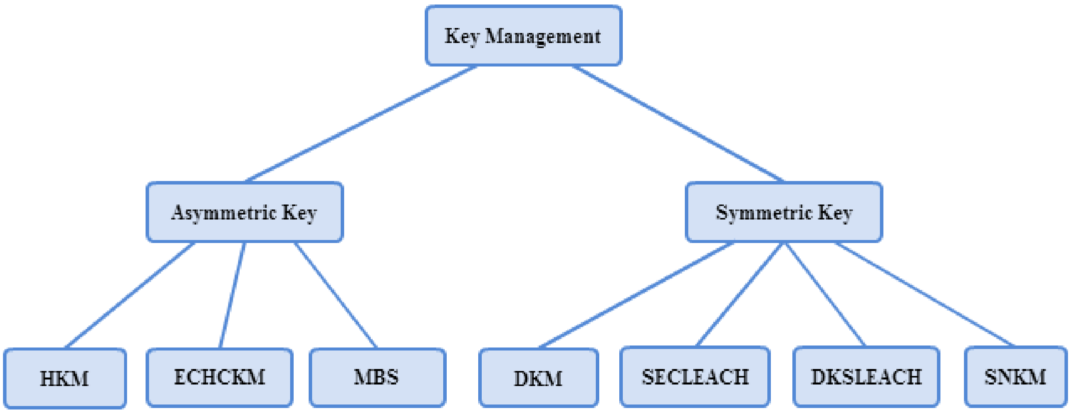

Fig 1 Classification of cluster-based key management schemes

3.1 Schemes based on LEACH

Low-energy adaptive clustering hierarchy (LEACH)[2], is a protocol architecture for WSNs that provides good performance in terms of system lifetime, latency, and data quality using energy-efficient cluster-based routing as well as media access along with application-specific data aggregation. LEACH includes a new, distributed cluster formation technique to save resources of nodes by dynamically forming cluster and electing different cluster head (CH) for each different round to evenly distribute work load and power consumption betweens sensor nodes.

As sensor nodes are unattended and at remote place, LEACH is also vulnerable to a number of security attacks [8], like jamming, spoofing, replay, etc. As in LEACH data aggregation and routing is carried out by CH, attacks on CHs are more damaging compare to other sensor nodes. If an intruder manages to become a CH, it can stage attacks such as sinkhole and selective forwarding, thus disrupting the workings of the network [8]. Even the intruder may try to inject bogus sensor data into the network.

LEACH is more robust against attacks than most other routing protocols [8]. In contrast to more conventional multi hop schemes where nodes around the base station (BS) are especially attractive for compromise. CHs in LEACH communicate directly with the BS, can be anywhere in the network, and change from round to round. All these characteristics of LEACH create difficulties to identify and compromise strategically more important nodes.

Due to the benefits of LEACH like provide less overhead, latency, increases network life time and data quality. So different versions of LEACH have been proposed, to enhance the security of LEACH, one of them is LEACH with security (SecLEACH)[3], which is based on random key pre distribution, which is used to secure CH-node communication in LEACH. This scheme protects the network from attacks by outsiders.

SecLEACH proposes to secure LEACH by using a probabilistic scheme. In SecLEACH, each node has K pre-distributed keys obtained randomly from a set of keys P. The main advantage provided by SecLEACH is the possibility to authenticate and to secure the communication between CH and cluster's members without the participation of the BS. Note that, the authors of SecLEACH have already proposed in [9] a protocol, called S-LEACH, in order to secure LEACH. SecLEACH is an improvement of S-LEACH. Since there are only two keys per node, S-LEACH does not provide a complete and efficient solution to node-to-CH authentication as said in [3].

3.2 Security node-based key management protocol

Another scheme is security node-based key management protocol (SNKM)[1], proposed for cluster-based sensor networks. Sensor nodes and CHs are responsible for data collection and transmission and Security nodes are responsible for key management. Security nodes restrain key management function of CHs, and reduce damage if CH is captured. Performance analysis and simulation shows that the SNKM consumes less energy, specially by CH as the work of key management is carried out by Security nodes, and therefore its delay time of key generation is short. At the same time, the SNKM also provides more collaborative authentication security for keys. It has strong resilience against node capture, and can support large scale network.

In SNKM, for each cluster they are electing a secure node on the bases of random number, generated through random function. If the random number is more than the predefined threshold value then sensor node is a candidate for security node. The work of security node is to elect CH as well as distribute keys and broadcast message to sensor node in cluster. For securing communication in SNKM pair-wise key has been used and for each CH, cluster key is generated for authentication using uTESLA, classic authentication protocol is used. Even security nodes monitor CHs and if abnormal behaviour found it start the election of new CH immediately.

Though, SNKM is efficient key management scheme and having a resistance against capture node, the problem with SNKM is that it is applicable on static network only and it is not scalable. That is because of the pair-wise key establishment between each pair of sensor node , if there are so many sensor node in neighbourhood it will be difficult to store the key in memory. Even malicious node may get elected as a CH or as security node that can expose whole cluster and eventually whole network.

3.3 Distance-based key management

Different from all the discussed key management schemes, distance-based key management (DKM)[10] is location dependent key management scheme , which distributes key based on distance that is hop count. It reduces the overhead by localizing the key things. In this scheme the election of the CH carried out in traditional way on the basis of the energy of sensor node. After that CH gets the distance of all nodes in cluster with help of acknowledgement packets. Using this distance CH generates the keys for nodes. Different key will be generated based on the different distance. So several security key will be generated based on the different security belts.

Here in DKM, key of the adjacent node would be same. So that it is possible to communicate with each neighbouring node without any extra overhead. Even use of nonce prevents hello flood attacks. And because of localization energy consumption is less. But the issues with DKM remain same which were there in LEACH. Like, it cannot prevent malicious node to be elected as a CH. Even a node in same security belt, which is compromised, can expose all the communication of that security belt. So DKM has major issues when it comes to security. Even the protocol is not scalable so cannot be applicable for large network.

3.4 Deterministic key management scheme for securing cluster-based sensor network

Deterministic key management scheme for securing cluster-based sensor network [5] uses DKS-LEACH protocol. This protocol enhances the security of LEACH protocol by not electing any malicious node as a CH. This approach prevents election of untrustworthy cluster head by checking its id at BS.

To make it more secure and reduce the communication overhead they have used deterministic key distribution approach over probabilistic one. As it reduces the message exchange for key establishment but increases the computation time that is at the BS and as we all are aware in case of WSN computation requires less energy compare to message exchanges.

DKS-LEACH architecture consist of two types of keys: (i) pair wise key shared between BS and CH (ii) Cluster' key, shared between sensor node and the CH that form the same cluster.

Thus using above algorithm, one can establish pair wise and cluster key for WSNs to make it secure. Even malicious node cannot be elected as a CH, as when CH sends request for pair wise key establishment to BS it also send its id to BS. So BS verifies the id of CH using data stored at BS and verifies the CH. Thus no malicious node can be selected as a CH. So by avoiding malicious node to be selected as CH, we can prevent sink hole and selective forwarding attacks. This protocol uses hash function, MAC function as well as nonce which provides authentication, integrity, confidentiality and also the freshness of messages to avoid eavesdropping attack.

In this approach at most three different key are stored at nodes so it minimize the memory usage also. Above approach reduce end-to-end for network with any no. of nodes but still energy consumption is a major issues in DKS-LEACH. Even there can be attack possible on WSN if sensor node or BS is compromised so scheme can be improved by making the network self resilient.

3.5 An Elliptic curve based Hierarchical cluster key management

Security is a major concern in WSNs, An Elliptic curve based hierarchical key management (ECHCKM)[11] achieves same level of security as other schemes but with help of smaller key size. In this scheme Elliptic curve cryptography is used compared to RSA for public key encryption as it provides same level of security with lesser key size. This scheme consists of three algorithms to establish keys between sensor nodes within cluster, keys between CHs and global key generation. This consist of static cluster formation scheme and generates a key at root CH(RCH) with less processing time. Though it is secure against snooping and modification attack but still once sensor node is compromised it may lead to compromise the whole cluster.

3.6 Hybrid key management scheme with double CH

In [12], authors have proposed a scheme to increase the life time of WSN by increasing the efficiency of network using double CH. In this hybrid key management (HKM) scheme another CH is selected which is responsible for safety of the nodes in cluster if in case CH becomes invalid. So this scheme increases security and also improves efficiency of network. Using this scheme one can achieve full network connectivity but still it is prone to attacks and not that much resilient.

IV. Comparison of different Techniques

This section shows comparison of previously discussed schemes. Table-1 shows comparison of different schemes based on parameters as follows. *Dynamic/Static* is whether a network formation is dynamic or not. *Resilience* i.e. if node is compromised how much damage is done to entire network. *Scalability* is measured in terms of number of nodes can be expanded in network. *Connectivity* refers to a level at which each node can communicate with other node. And efficiency is already explained in detail in evaluation metrics.

Table-1 Comparison of different key management techniques for Clustered based WSNs

Name	*Dynamic/Static*	*Resilience*	*Scalability*	*Connectivity*	*Efficiency*
LEACH	D	No	Yes	100%	Yes
SecLEACH	D	Less	Yes	Not 100%	Yes
SNKM	S	More	No	100%	Yes
DKM	S	Less	No	Not 100%	Yes
DKS LEACH	D	Less	Yes	100%	No
ECHCKM	S	More	No	100%	No
HKM	D	Less	Yes	100%	Yes

V. Conclusion

We have so far discussed various key management techniques for clustered based wireless sensor networks. With wide verities of application of WSNs where security is major concern, key management is grasping more and more attention. So many schemes have been published by many researchers. Some of which we have mentioned in our work. From that we can conclude that for the specific application and requirement one scheme is batter over other but as a whole none of the scheme fulfills all the evaluation metrics. So we can conclude that not a single scheme, mentioned above, satisfy all evaluation metrics. So using this work one can get encouragement to develop new scheme that may satisfy the need.

REFERENCES

[1] B Jiana and E Xu, "An Energy-efficient Security Node-based Key Management Protocol for WSN," In : 2nd International Symposium on Computer , Communication, Control and Automation. 2013.

[2] WB Heinzelman, AP Chandrakasan and H Balakrishnan, "An Application-Specific Protocol Architecture for Wireless microsensor networks," In: IEEE Transactions on Wireless Communications. vol. 1. October 2002, pp.660–670.

[3] MB Leonardo, O Hao and C Wong, "Secleach: A Random Key Distribution Solution for Securing Clustered sensor networks," In: IEEE Network Computing and Application, April 2006, pp.145-154.

[4] I Gupta, D Riordan and S Sampali, "Cluster-head Election using Fuzzy Logic for Wireless Sensor Networks," In: Communication Networks and Services Research Conference IEEE 2005, pp.255-260.

[5] M Ba, I Niang and B Gueye, " A Deterministic Key Management Scheme for Securing Cluster-based Sensor Networks," In : 8th International Conference on Embedded and Ubiquitous Computing IEEE 2010, pp. 422-227.

[6] X He, M Niedermeier and H Meer," Dynamic Key Management in Wireless Sensor Networks:A survey," In: Journal of Network and Computer Applications, pp.611-622. 2012.

[7] Simplicio Jr MA, Barreto PSLM, Margi CB and Carvalho TCMB, "A survey on key management mechanisms for distributed wireless sensor networks," In: Computer Networks 2010.

[8] C Intangonwaiwat, R Govindan and D Estrain, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," In : Proceeding Fourth Annual ACM International Conference in Mobile Computing and Networking . Boston, Aug. 2000, pp.56-67.

[9] OHW Ferreira and Vilaca and Loureiro, " On the security of clusterbased communication protocols for wireless sensor networks," In : Proceedings of Internation conference of Computer Networks. April 2005, pp. 449–458.

[10] Zhang YY ,Li XZ,Cao, JP,Zeng, LK,Zhen Y and Gao DQ, " Distance-Based key management in Hierarchical Wireless Sensor Network," In : International Conference on Automatic Control and Artificial Intelligence IEEE 2012,pp.915-918.

[11] S Sahoo and M Sahoo, "An elliptic curve based hierarchical cluster key management in wireless sensor network," In International Conference on Advanced Computing, Networking, and Informatics (ICACNI '13), June 2013.

[12] M Hongbin,W Yingli,Y Shuang,Y Hai and L Zhenhai, " Hybrid key management mechanism based on double cluster head structure," In : 2nd International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012, IEEE, pp.1164-1167.

[13] Jennifer Yick, Biswanath Mukherjee and Dipak Ghosal, "Wireless sensor network survey," In:Computer Network 52, 2008, pp.2292-2330