American-Eurasian Journal of Scientific Research 11 (1): 63-71, 2016
ISSN 1818-6785

DOI: 10.5829/idosi.aejsr.2016.11.1.22829

Service Orient Stream Cipher Based Key Management Scheme for Secure Data Access Control Using Elliptic Curve Cryptography in Wireless Broadcast Networks

[1]D. Geetha and [2]Dr. S. Sakthivel

[1]Research Scholar, Assistant Professor/CSE,
Adhiyamaan College of Engineering, Hosur-635 109, India
[2]Professor/CSE, Sona College of Technology, Salem-6, India

Abstract: Wireless broadcast network has various services being transmitted in the network, which can be received by various users based on their registration and possession of the keys. There are many approaches has been discussed in the literature which suffers with the problem of overhead in generating in keys and distributing them to the users of the network. We propose a novel approach, which generates keys based on services and distribute them to the user who have been registered. For each service being available in the network, the controller generates a group key which is unique for the service users which is generated using elliptic curve cryptography and proposes a stream cipher based hash function which generates the key for the service stream and will be unique and useful for only the concern stream. The key will be changed for each stream of the service data which can be computed with the help of previous stream keys and values of elliptic curve. The proposed method has reduces the overhead of key generation and distribution to the users and the method has reduces the time complexity also.

Key words: Wireless Broadcast Networks · Key Management Scheme · Service Orient Stream · Data Access Control

INTRODUCTION

Wireless broadcast networks are the collection of wireless nodes which is geographically spread into many kilometers and has a base station which broadcasts the data packets into the network and the nodes of the network can receive the packets broadcasted. The thing is in order to decrypt and see the content of the packet being received the wireless client node must possess the decryption key. For example in any television network, there are number of channels being available and broadcasted by the base station and the wireless nodes has to registered to the base station or the controlling station. Whatever the channel being transmitted, the client nodes can receive and see the content of the packet only with the possession of the key being used for decryption [1].

To provide secure data access control there are many access restriction protocols has been discussed. The key based data access is one among them, that the user who have the key only can access the data packets. The authorized users will be assigned with a secret key for encryption using which the user can access the data stream. Sometimes there are users who move from different groups like changes the channel selection. So that the user has to be restricted from accessing the previously registered service data packets. This requires more strategic method of key management has to be used [2].

The rigidity of elliptic curve cryptography is well known because it is very hard to compute the key even if it has been caught by any malicious node in between any transmission. The pure ECC will not be effective in real time wireless broadcasting due to the time complexity of

Corresponding Author: D. Geetha, Research Scholar, Assistant Professor/CSE,
Adhiyamaan College of Engineering, Hosur-635 109, India.

the key generation and the same can be adapted with little changes to support wireless broadcast networks in a service orient architecture [3].

In television network the subscriber has to register and subscribe the channel so that he can receive and decrypt the content of the channel. How this is performed is by using some key management mechanisms. The broadcasting node maintains various keys for each of the channel or the packet being transmitted like encryption and decryption. Based on the key being used for encryption and decryption the packet content may be visited by the receiving nodes of the network. There are many key management mechanisms has been introduced earlier for the broadcasting network like group key management, public-private key based mechanisms and session based approaches and so on. Whatever it may be, the problem of network overhead introduced by generating the keys and distributing them to the nodes of the network and computation cost is also higher [4].

The service orient stream represents the content of each channel in the wireless broadcast networks, for each service available in the network, there will be an unique key will be used by the network and the user will be given with the service key at the registration phase and at the starting of each stream part an new key will be generated for encryption and the decryption key could be generated or identified by the client itself using the earlier part of the stream key. By identifying the stream key being used to perform encryption, the decryption key could be identified by the client to perform decryption of pay load data [5].

Related Works: There are many approaches has been discussed to perform secure communication in wireless broadcast networks and we discuss few of them here for better understanding.

An Efficient Key Management Scheme for Secure Data Access Control in Wireless Broadcast Services [1], propose an efficient key management scheme (namely KTR) to key distribution with regarding too complex subscription options and user activities. KTR has the following advantages. First, it supports all subscription activities in wireless broadcast services. Second, in KTR, a user only needs to hold one set of keys for all subscribed programs, instead of separate sets of keys for each program. Third, KTR identifies the minimum set of keys that must be changed to ensure broadcast security and minimize the rekey cost. Our simulations show that KTR can save about 45% of communication overhead in the broadcast channel and about 50% of decryption cost for each user, compared with logical key hierarchy based approaches.

Enabling end-to-end secure communication between wireless sensor networks and the Internet [2], propose an end-to-end secure communication scheme for W2T in WSNs in which we follow an asymmetric approach for authentication and key management using signcryption and symmetric key encryption. In our proposed scheme, a great part of the work for authentication and access control is shifted to a gateway between a WSN and the Internet to reduce the burden and energy consumption in the sensor nodes. In addition, our scheme can ensure the privacy of user identities and key negotiation materials and denial of service (DoS) attacks targeted at the sensor nodes can be effectively blocked at the gateway. We will also conduct quantitative analysis and an experiment to show that our proposed scheme can enhance the effectiveness of end-to-end security while reducing the cost of sensor nodes in terms of computation, communication and storage overhead as well as the latency of handshaking compared to similar schemes that are based on Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols [6].

Key management protocol with end-to-end data security and key revocation for a multi-BS wireless sensor network [3-10], propose a large-scale wireless sensor network with multiple base stations (BS), a key management protocol is designed. For securely relaying data between a node and a base station or two nodes, an end-to-end data security method is adopted by this protocol. Further employing a distributed key revocation scheme to efficiently remove compromised nodes then forms our key management protocol celled multi-BS key management protocol (MKMP). Through performance evaluation, we show that MKMP outperforms LEDS Ren *et al*. (IEEE Trans Mobile Comp. 7(5): 585–598, 2008) in terms of efficiency of resilience against the node capture attack.

A key management and secure routing integrated framework for Mobile Ad-hoc Networks [11], propose a KM–SR integrated scheme that addresses KM–SR interdependency cycle problem. By using identity based cryptography (IBC), this scheme provides security

features including confidentiality, integrity, authentication, freshness and non-repudiation. Compared to symmetric cryptography, traditional asymmetric cryptography and previous IBC schemes, this scheme has improvements in many aspects. We provide theoretical proof of the security of the scheme and demonstrate the efficiency of the scheme with practical simulation

Mitigating jamming attacks in wireless broadcast systems [12], propose a novel scheme with random channel sharing. This scheme reduces the communication cost from 2t to (1 + p)t extra copies, where p determines the channel sharing probability ($0 < p < 1$). In addition, it does not increase the hardware complexity as it does not require a receiver to operate on multiple channels at the same time.

Randomized differential dsss: Jamming-resistant wireless broadcast communication [13], propose a Randomized Differential DSSS (RD-DSSS) scheme to achieve anti-jamming broadcast communication without shared keys. RD-DSSS encodes each bit of data using the correlation of unpredictable spreading codes. Specifically, bit "0" is encoded using two different spreading codes, which have low correlation with each other, while bit "1" is encoded using two identical spreading codes, which have high correlation. To defeat reactive jamming attacks, RD-DSSS uses multiple spreading code sequences to spread each message and rearranges the spread output before transmitting it. Our theoretical analysis and simulation results show that RD-DSSS can effectively defeat jamming attacks for anti-jamming broadcast communication without shared keys.

A Secret Sharing-Based Key Management in Hierarchical Wireless Sensor Network [14, 15], resent a Secret sharing-based key management (SSKM). SSKM utilizes the advantages of hierarchical architecture and adopts two-level key management and authentication mechanism, which can efficiently protect the allover network communication security and survivability. Different from previous works, the SSKM distributes keys based on secret sharing mechanism by the clustered architecture, which not only localizes the key things but also keeps scalability. The SSKM provides various session keys, the network key for base station (BS) and cluster heads (CHs); the cluster key between the cluster head and member nodes. The SSKM dynamically generates different keys based on different polynomials from BS in different periods which can protect the network from the compromised nodes and reduce the high probability of the common keys. The security analysis shows that the SSKM can prevent several attacks effectively and reduce the energy consumption.

In [16], the authors present a low-cost secret-sharing scheme for sensor network. This paper provides basic building blocks to establish secure communication through exchanging secret keys between neighbor nodes without any cryptography methods. In [5], authors also design a second algorithm which extends the secret key establishment. However, due to the exchange happening among sensors, it consumes lots of energy. Moreover, the authentication between neighbor nodes also needs to exchange large messages, which makes it unsuitable for wireless sensor network.

A distributed group rekeying scheme for wireless sensor networks [17, 18], propose a group key distribution scheme for WSNs in the IoT scenario in which we organize sensor nodes into groups in a hierarchical structure. In the upper wired layer, an end-to-end secure communication protocol is used to distribute group keys for subgroups to the trusted head nodes and the head nodes then distribute the group keys through underlying tree-based topology and wireless multicast to minimize energy consumption. We also perform some quantitative analyses as well as experiments to show that our proposed scheme is secure and has t-revocation capability. The total cost of distributing and rekeying the group keys is also analyzed and compared to that in some other comparable schemes.

All the above discussed approach has the problem of network overhead introduced by broadcasting the keys to the users of the network and the computation cost of the keys also higher. The methods also introduce higher time complexity and increases the key distribution cost also.

Proposed Method: The proposed approach has different stage of secure broadcasting namely Service Orient Key Generation and Distribution, Stream Cipher Hash Function, Encryption, Decryption. We discuss each of the functional components in detail in this section here.

The Figure 1 shows the architecture and functional components of the proposed system and will be explained in detail here in this section.

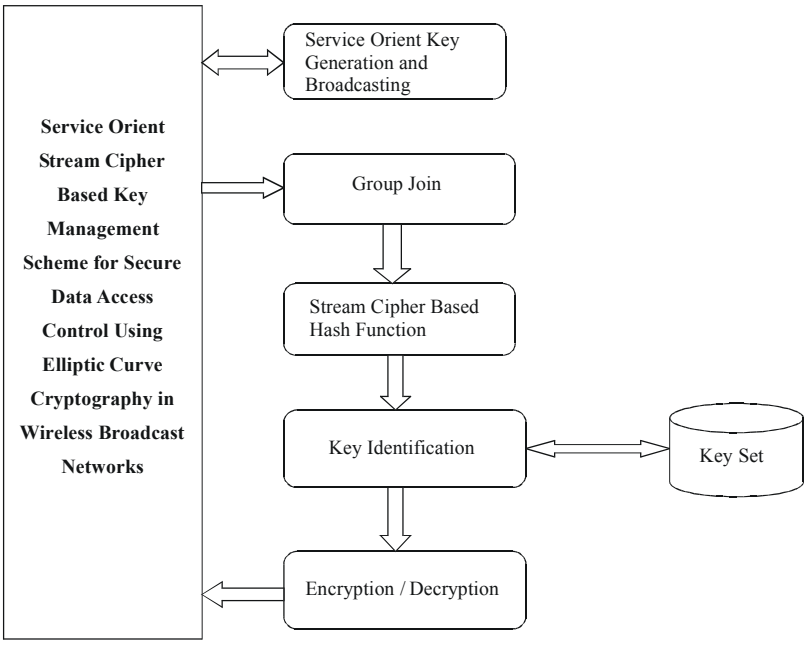


Fig. 1: Proposed System Architecture

Service Orient Key Generation and Distribution: The proposed method generates unique key Sk, for each of the service packets the controller or the base station generates the key and broadcast into the network initially and whatever the nodes present in the network could receive the keys by the nodes and will use to perform encryption and decryption at the next stages. For each service available, the base station generates the key and broadcast the packets into the network which can be received by the nodes or users of the network.

Algorithm:
Input: NULL
Output: Service Key Set SKS.
Step1: start
Step2: Initialize Service set Ss.
Step3: Identify set of all services available.

$SS = \int \sum Service \in Network$

Step4: for each service Si from SS
Initialize service Id SID.

Compute maximum bytes of streams to be attached.

$$Ms = \frac{Bandwidth}{size(SS)} \times ServicePriority$$

Generate Encryption key Ek using elliptic curve cryptography.

Cs = compute current size of the stream using prime factor.

$$SID = SID+MS+CS.$$

Perform Encryption Cipher = Encrypt(SID, EK).
Store Cipher, SID, EK to the key set.
SKS = {Cipher, SID, EK}.
End
Step3: stop.

Group Join: Group join is the process of joining the network by the client nodes. Whenever the client node generates the group join request the controller sends the service being requested and the service id and the encryption key in a secure channel to the user. By receiving these two information, the clients perform decryption of the service key using the key being provided and identify the payload length of the current service stream [19-23].

Algorithm:
Input: Null
Output: Service ID, Stream Size, Current Size.
Step1: start

Step2: Generate group join request GJOIN = {Service Name}.
Step3: Receive Reply GJREPLY.
Step4: Receive key Ek.
Step5: Cipher cp = GJREPLY(payload).
Step6: Text t = Decrypt(cp,Ek)
Step7: Identify service id SID, ML, Cs = Extract(t).
Step8: stop.

Stream Cipher Based Hash Function: The stream cipher based hash function performs the encryption and decryption of stream at each time. The method computes the prime factor and verifies whether it comes within the boundary of maximum stream size. Based on the identified stream size the data is encoded into the packet and broadcasted into the network.

Algorithm:
Input: NULL
Output: packet p
Step1: start
Step2: Identify the service key parameters.

SID = SID.Service ϵ Keyset Ks.

Step 3: Identify the maximum stream size Ms = $\int Ms(SID) \in Ks$
Step4: Identify the current size Cs = $\int Cs(SID) \in Ks$
Step5: Ek = Identify the key by identifying the number from the curve.
Step5: Read stream size with Cs and encrypt with packet P.
Step6: Broadcast packet p.
Step7: stop.

Key Identification: The key identification is performed based on the service key Id present in the service packet. From the service id being available in the packet, the client or the user will identify the keys using which the stream has been encoded and decrypted using the key received at the time of group join.

Algorithm:
Input: Packet P.
Output: Max Size ms, Current size Cs.
Step1: start
Step2: Extract Service id SID = P.SiD
Step3: Decrypt SID with key Ek.
Step4: Ms = second two bytes of SID.
Step5: Cs=Third two byte of SID.
Step6: Identify the value of the curve at Cs = $\int_{i=1}^{size(curve)} Curve(cs)$

Step7: stop.

Encryption Decryption: The service provider or the base station generates the packet using the maximum stream size and the current stream size of the service. According to the size of streams, the stream data is read and encrypted with the key for the service and broadcast into the network. The client node which receives the packet, extract the service id and decrypts the sid to identify the maximum stream and current stream size. According to the size identified, the payload being extracted and decrypted using the key Ek.

RESULTS AND DISCUSSION

The proposed method has been implemented and tested with number of groups and many number of users of the groups with S number of services available in the network. The proposed method has produced efficient results with different number of services and the number of users available in the network. The method generates different number of stream size according to the bandwidth condition and selects a prime value which is used to select the number of stream size used to generate the packet.

Unlike other methods the method does not send number of keys to the network and does not broadcast number of keys into the network. It broadcast a single multi slot key to the network at each session and the rest is performed by the user itself. So the cost of key distribution is less compare to other schemes. The cryptanalysis can be performed to measure the performance and efficiency of the proposed service orient stream cipher based key management scheme.

In general cryptography there are two types of ciphers has been used namely stream and block ciphers. The earliest methods have used any of the above said schemes to perform cryptography. But the proposed approach has utilized both steam and block based ciphers in different situations. For the key generation and distribution the approach has used block based cipher whereas for the real communication the method has used stream ciphers.

The efficiency in security of the protocol can be measured using various strategic measures like confidentiality, Forward secrecy, computation and communication overhead.

Confidentiality: The method generates unique key for each service available in the network and broadcast them into the network which can be received by all the nodes within the network. But how the confidentiality is maintained is, even the node receives the service key it cannot decrypt the key to get the original service key. The key generator uses different stream size at different session based on the point get selected in the key generation process. The node will get to know only by performing group join with the key generator, which contains the decryption key and the current stream size. This makes the key as more confidential one. Because the node will be given with the decryption key and the current stream size and the key itself has the detail of the current point has been selected in the Elliptic Curve. This will be changed at each time window for each service by the key generator which increases the tampering quality of the proposed protocol. This ensures that the node which does not possess the proper key cannot read the original content because the key has the length of payload and the point has to be used to get the decryption key and so on.

Forward Secrecy: The node which leaves the group could never use the key for long time because at the each session of time window the service orient key will be modified and broadcasted to the users. The key only has the current stream size, point to be selected to compute the decryption key and so on. This will be given to the node which are located within the region of the network or in the group.

Backward Secrecy: The earlier user may possess the previous key but the method generates different key at different time window which will be given only to the users in current group. Even the user posse's earlier key, he cannot identify what the stream size, which is the point to be used to get the decryption key from the elliptic curve. The tampering quality of elliptic curve supports here because it is not such easy for the malicious user to try number of times and get the exact point to compute the decryption key. Also the time complexity will be higher to put such trial in finding the exact key and the session time may be expired before that.

Performance Analysis: The earlier approaches used various key generation mechanism which need number of keys to be generated and distributed to the user. Still the malicious user can easily identify or the user present in earlier stage can still compute the decryption key to get the original information. But in our protocol, the user cannot do like the previous one, because the protocol chooses different stream or payload length at different time window to compute the service key, which is selected from the elliptic curve and cannot be judged by any user out of group. This definitely increases the performance of the protocol in all the factors of cryptanalysis.

Storage Overhead: The method uses only one two key at any time, one for the group key and another one for the service. Even the service key will be replaced at each time window by the new key provided for the service being available. This reduces the storage overhead than the other methods.

Computation Overhead: The genuine node can easily compute the decryption key because, there is only two stage in getting the decryption key. One is, getting the point specified in the service key, the node has to get the value present in the point from the elliptic curve then compute the key for decryption. The computation overhead is hugely reduced and comparatively less than other approaches.

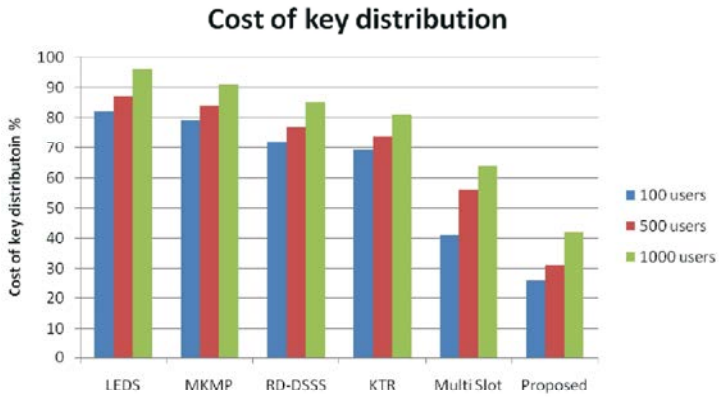
Communication Overhead: Unlike other methods the method does not send number of keys to the network and does not broadcast number of keys into the network. It broadcast session based service key to the network at each session and the rest is performed by the user itself. So the cost of key distribution is less compare to other schemes.

The graph 1, shows the comparison of cost occurred in key distribution and it shows clearly that the proposed method has produced less cost than others.

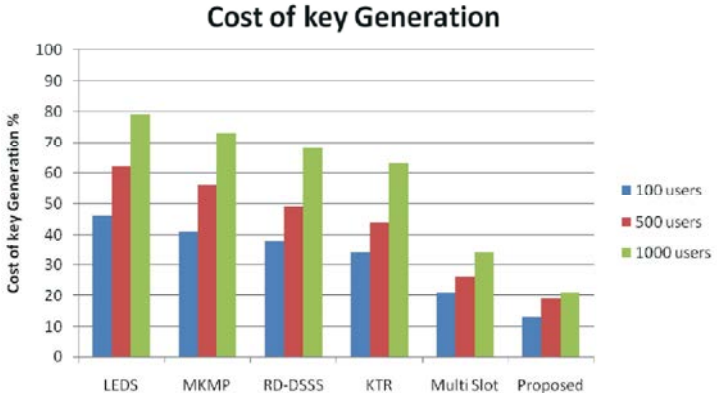
The graph2 shows the comparison of cost occurred in the key generation process and the result shows that the proposed method has produces less cost than others.

The Graph 3, shows the tampering efficiency of the different methods and it shows clearly that the proposed method has more tampering efficiency than the other method.

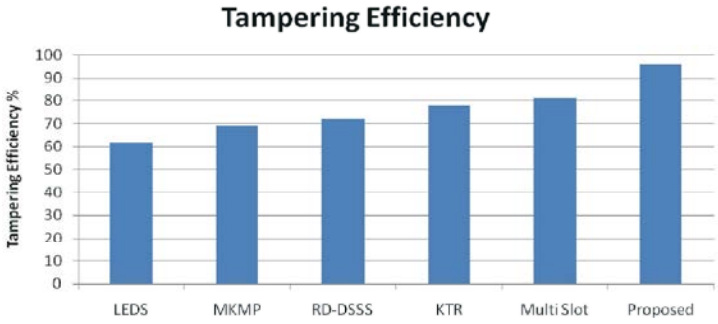
The Graph 4, shows the comparative analysis on computation and distribution overhead produced by the different methods and it shows clearly that the proposed method has produced less overhead than other methods.



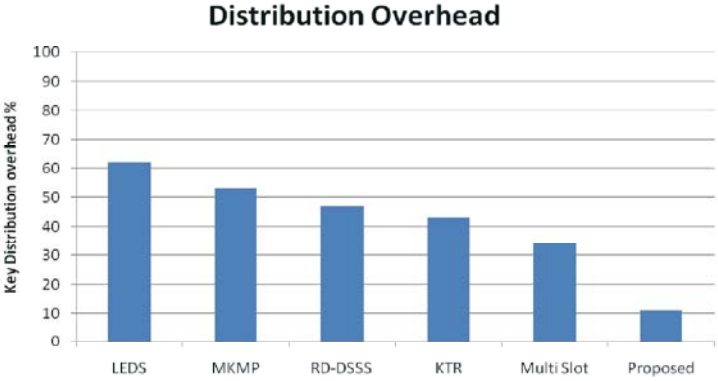
Graph 1: Comparison of cost of key distribution



Graph 2: comparison of cost occurred in key generation.



Graph 3: Comparison of tampering efficiency



Graph 4: Comparison of key generation and distribution overhead

CONCLUSION

In this paper we proposed a stream cipher based key management mechanism for wireless broadcast networks. The method generates different maximum stream size and current stream size for each service available in the network. The generated service id is distributed to the users who have been registered with the base station. From the service id and the key being distributed the user can identify the stream size maximum and the current stream size. With the current stream size, the decryption key is identified from the elliptic curve and the value present at the location of the curve is the decryption key. Based on identified stream size, the payload data is extracted and decrypted using the key being identified from the elliptic curve. The method selects the stream size different at each time or for each packet which improves the security of the overall transmission. The method selects different stream size and according to the stream size a key from the elliptic curve is selected to perform encryption which is identified by the receiver also in a secure manner. Also there is no key generation and transmission for each session or the transmission. The method reduces the problem or overhead of key distribution and key generation cost and reduces the time complexity also.

REFERENCES

1. Rajesh, K.V., 2012. An Efficient Key Management Scheme for Secure Data Access Control in Wireless Broadcast Services international Journal of Smart Sensors and Ad Hoc Networks,(IJSSAN) , 1: 4.
2. Hong Yu, Jingsha He, Ting Zhang, Peng Xiao and Yuqiang Zhang, 2013. Enabling end-to-end secure communication between wireless sensor networks and the Internet, World Wide Web, 16(4): 515-540.
3. Cao, X., W. Kou, X. Zeng and L. Dang, 2009. Identity-based anonymous remote authentication for value-added services in mobile networks. IEEE Trans. Veh. Technol, 58(7): 3508-3517.
4. Christophe, B., 2011. The web of things vision: things as a service and interaction patterns. Bell Labs. Tech. J., 16(1): 55-62.
5. Granjal, J., E. Monteiro and J.S. Silva, 2010. A secure interconnection model for IPv6 enabled wireless sensor networks. In: Proceeding of the 2010 IFIP Wireless Days, Venice, Italy, pp: 1-6.
6. Gupta, V., A. Poursohi and P. Udupi, 2010. Sensor network: an open data exchange for the web of things. In: Proceeding of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops, Menlo Park, California, pp: 753-755.
7. Mzid, R., M. Boujelben, H. Youssef and M. Abid, 2010. Adapting TLS handshake protocol for heterogeneous IP-based WSN using identity based cryptography. In: Proceeding of the International Conference on Wireless and Ubiquitous Systems, Sousse, Tunisia, pp: 1-8.
8. Roman, R., 2011. Key management systems for sensor networks in the context of the internet of things, Comput. Electr. Eng, 37(2): 147-159.
9. Yu, H. and J. He, 2012. Trust-based mutual authentication for bootstrapping in 6LoWPAN. J. Commun. Technol, 7(8): 634-642.
10. Huei-WenFerng, Jeffrey Nurhakim and Shi-Jinn Horng, 2014. Key management protocol with end-to-end data security and key revocation for a multi-BS wireless sensor network, Springer, Wireless Networks, 20(4): 625-637.
11. Shushan Zhao, 2013. A key management and secure routing integrated framework for Mobile Ad-hoc Networks, Elsevier, Ad Hoc Networks, 11(3): 1046-1061.
12. Dong Qi, Donggang Liu and Matthew Wright, 2013. Mitigating jamming attacks in wireless broadcast systems, Springer, Wireless Networks, 19(8): 1867-1880.
13. Liu, Y., P. Ning, H. Dai and A. Liu, 2010. Randomized differential dsss: Jamming-resistant wireless broadcast communication. In Proceedings of the 29th IEEE international conference on computer communications (INFOCOM').
14. Liu, D., J. Raymer and A. Fox, 2012. Efficient and timely jamming detection in wireless sensor networks. In Proceedings of IEEE international conference on mobile ad hoc and sensor systems (MASS).
15. Zhang Yiying, Chunying Wu, Jinping Cao1 and Xiangzhen Li, 2013. International Journal of Distributed Sensor Networks.
16. Bertier, M., A. Mostefaoui and G. Trédan, 2010. Low-cost secret-sharing in sensor networks, in Proceedings of the IEEE 12th International Symposium on High Assurance Systems Engineering (HASE '10), pp: 1-9.

17. Claveirole, T., M. Dias De Amorim, M. Abdalla and Y. Viniotis, 2008. Securing wireless sensor networks against aggregator compromises, IEEE Communications Magazine, 46(4): 134-141.
18. Seyed, H.N., H.J. Amir and D. Vanesa, 2011. A distributed group rekeying scheme for wireless sensor networks, in Proceedings of the 6th International Conference on Systems and Networks Communications (ICSNC '11), pp: 127-135.
19. Zhang, Y.Y., X.Z. Li, J.M. Liu, J.C. Yang and B.J. Cui, 2012. A secure hierarchical key management scheme in wireless sensor network, The International Journal of Distributed Sensor Networks, 7471: 8.
20. Zhang, Y.Y., X.Z. Li, J.C. Yang, Y.A. Liu, N.X. Xiong and A.V. Vasilakos, 2012. A real-time dynamic key management for hierarchical wireless multimedia sensor network, Multimedia Tools and Applications.
21. Agrawal, S., 2012. Verifiable secret sharing in a total of three rounds, Information Processing Letters, 112: 856-859.
22. Hua, C., X. Liao and X. Cheng, 2012. Verifiable multi-secret sharing based on LFSR sequences, Theoretical Computer Science, 445: 52-62.
23. Liu, Y.X., L. Harn, C.N. Yang and Y.Q. Zhang, 2012. Efficient secret sharing schemes, Journal of Systems and Software, 85(6): 1325-1332.