A Triplet key approach or confidentiality in dynamic wireless sensor networks.

J. Lekha

ABSTRACT

These are several methods of exchanging secret keys among the systems on the wireless sensor network. Because of its high chance of vulnerability most of the existing methods have security against only any one of the security mechanisms but not all. So we propose a multi secure approach which combines more than one protection mechanism. The aim of this approach is to distribute secret keys among the nodes on dynamic wireless sensor networks called Network Coding Approach. Existing methods for distributing keys in static wireless sensor networks which does not have extensibility. They are

1) Public key distribution
2) KDC
3) Key Predistribution.

The drawback of existing static method is that it creates network traffic when the existing predistributed keys have been exhausted. The server node is subjected to single point of attack which results in failure of network. We extend one of the existing methods along with the proposed system. The proposed coding approach of achieving security mechanisms contain 1) client to server pairwise key distribution, 2) mutual key distribution, 3) node blocking. The server S node bootstraps the network and act as key enabler. We concentrate on authentication of server node for some single point of attack. Thus the approach is said to prove in confidentiality, authentication and also reliability. Our results include performance evaluation with other existing mechanisms such as Hybrid approach; Tree based approach and using some security metrics and resource utilization it is proven to be best.

Keywords: KDC, Public keys, Wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks Fig 1 are easily open for unauthorized access. Many corporate users have started using Wireless LAN to decrease their investment in wired setup and to increase data transmission rate. Another reason for users preferring wireless network is it can include more coverage area than a wired network. The basic requirement to enjoy all these advantages is to have a wireless card on your PC, Laptop or a mobile phone and a Access Point in your Wireless LAN. This can also be extended to Wireless WAN. Apart form all these advantages it has equivalent disadvantages. Even though people form small petty shops to large super computers have started using wireless networks the security mechanism for these networks should be at a greater level. You have to make some security configuration settings and IP configuration after setting your Wireless network.

Therefore Wireless WAN should also possess all the security services such as confidentiality, authentication, integrity, non-repudiation and availability which results in a low-latency and secure systems.

Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore (saran.lekha@gmail.com)

Existing methods of providing security are analyzed and categorized into three types 1. Public key distribution using basic symmetric key cryptography 2. Session key distribution using KDC 3.Using Key Pre-Distribution Scheme. We first consider the method of public key distribution is that it requires huge transmission of data and cipher key of equal length to that of plain text on the network. Also it is prone to man in the middle attack. The second method is key distribution using KDC. Using KDC to share secret keys faces the problem of central point of attack. If the KDC is compromised then all the secret keys are easily captured. Also if a node wants to communicate with n nodes then the node requires 'n' different keys. If 'n' nodes want to communicate with N other nodes on the network then a total of n (n-1) keys are require. Therefore if one million people need to communicate with each other then each person requires one million keys, so in total one trillion keys are needed. This is called as n^2 problem because the number of keys required for n nodes is N^2. Another problem is key management by KDC and unsecure key distribution.

The third approach is key pre distribution 250 keys are pre distributed in each node out of total 100000 keys. But the network key is erased as long as the pairwise keys are established. So if a *node* needs to communicate with another node then it should use another network key. So this method is suitable only for static network but not to dynamic network.

Considering all the drawbacks of existing system the proposed system is designed with three layers of security discussed in the succeeding section.

II. Methodology

1) The proposed system ensures security along with the following properties:

- Focus on uniform distribution of secret keys.
- Extend the mobility of the server in wireless medium.
- Use a mobile node to bootstrap the network thereby providing global efficiency.
- Reduces the number of transmissions by storing limited number of keys.
- Blind key distribution.
- Key renewal capacity.
- Authentication of the server.
- Easy generation of mutual keys.
- Automatic node blocking in case of node compromise.
- Deterministic security.

The system ensures the three security mechanisms confidentiality, integrity and authentication of the server to client all together.

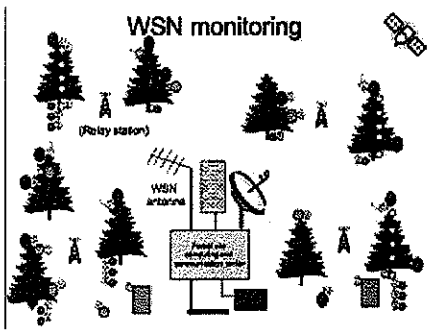


Fig 1: Representation of Wireless Sensor Network.

The proposed methods are:

- Client to server pairwise key disribution.(confidentiality)[1] [2] [3]
- Mutual key distribution

❖ Node blocking of compromised nodes.

The proposed coding approach of protocol [5] focuses on network layer since it is responsible for wireless communication as shown in fig 2.

Layer	Cryptographic System
Application	Kerberos
Transport	SSL/TLS
WAN e.g. Internet	IPsec
Data Link	PPTP, L2TP (really only a tunneling system)
Physical	Not applicable. No messages are sent at this layer—only individual bits

Fig 2: OSI layers and Cryptographic systems.

Distribution of pairwise keys in sample space.

Consider a communication in a sample space with two nodes A and B through a server S (maybe a mobile node). The following steps ensure secret distribution of pairwise keys.

Step 1: Generate a large pool of independent keys $k_1 \ldots k_i$ where $1<=i<=|P|-1$

Step 2: Produce a binary sequence equal to the key size by using Vegenere cipher 'R'.

Step 3: Find $k_i \oplus R$, encrypt and store it in S.

Step 4 : Each node is stored with C disjoint keys $C<|P|$. Let C be the number of links a node has in its lifetime.

Step 5: Then each node contains C disjoint keys from P along with their identifiers for each key.

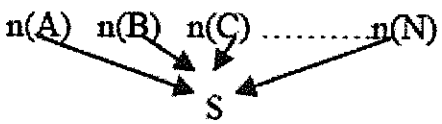
For $k_i \in n(A)$, $k_i \leftarrow id_i$

Step 6: The server sends a *Hello* message to all the nodes connected to it.

Step 7: The client node replies by sending its identifier of the chosen key from 'C' keys to the server

$$id_i, \in k_i, n(B)$$
$$n(A) \longrightarrow S$$

Step 8: Similarly all the client nodes will send its identifier if the chosen key to S.



Step 9: The server now performs a look up operation in its table of keys to find out the pairwise encrypted [4] key set $k_i \oplus$ of A and $k_i \oplus$ R of B which needs to communicate.

Step 10: This messages are conversely send to A and B.

$$nA(k_i \oplus R) \oplus nB(K_i \oplus R)$$

Step 11: The client nodes can now exchange the message using each other keys

$$E(K_i(A)[M_A \longrightarrow B]].\ E[K_1(B)\ [\ M_B \longrightarrow A]]$$

Large scale pairwise key distribution in real time systems

We introduce three keys namely a local identifier 'j', a node identifier 'nd' and global key identifier 'i'. The global key identifier is obtained by the concatenation of the local key identifier and the node identifier. Each node is provided with a node identifier and local identifier. The use of global key identifier is discussed later sections.

For example,

$|n|$ = 24 bits. $|j|$ = 8 bits.

Then,

$|i| = |n|*|j|$ = 32 bits (* represents concatenation)

Step 1: The sever node S sends Hello message to all the nodes on the network.

Step 2: Each node informs its availability on the wireless transmission range of the network by sending its node identifier 'nd' in a list of identifiers Ln in all its neighbours {nd, Ln } and in S.

Step 3: Thus the server receives this combination form all the client nodes on the wireless transmission range i.e $\{nd_A, L_{n(A)}\}, \{nd_B, L_B\}$...

Step 4 : The server checks if ,

$$nd_A \in L_{n(B)}$$

$$nd_B \in L_{n(A)}$$

Step 5: If this condition does not satisfy i.e nd_A,, nd_B the server sends to these client nodes the global key identifier i.

$$nd_A * j_A, nd_B * j_B$$

Step 6: XOR combination of the secret keys and its local identifiers are also send to the unsatisfied nodes.

$$k_A * j_A \oplus k_B * j_B$$

Step 7: Thus each node receives a pair of keys j,i with each other along with the keys K_i

Handling Key Exhaustion

We store C keys in each client node. When each node makes more than C links with other nodes then the prestored keys gets exhausted. In such case the client nodes can request for extra keys form the sever node.

Step 1: The client node sends request for additional keys by using Euclidean algorithm.

Step 2: The algorithm takes the GCD of the number of prestored keys and the number of nodes within the transmission limit.

Step 3: The resulting number of keys is requested form the server. For example assume that the client node requests for four keys form the server. The client sends one node identifier and four local key identifiers to the server.

$$n_{(A)}, \{5,6,13,15\}$$

Step 4: The server performs a look up operation and fetches the keys related to it.

Step 5: The server now generates four new keys using XOR operation of the Vegenere cipher with the existing four keys.

Step 6: The server now performs the following logical operation on the old and new keys

$$E(k_{n(A)} * 5 \oplus k_{n(A)} * 6 \oplus k_{n(A)} * 13 \oplus k_{n(A)} * 15)$$

Step 7: The server also authenticates itself by acknowledging the client nodes with the XOR combination of one esisting local key identifier and a new key

$$[5,17, k_{n(A)} * 5 \oplus k_{n(A)} * 1$$

Step 8 : The client node can request for new keys until it has existing local key identifiers.

Step 9 : To store new keys the client node can also delete existing local key identifiers.

Mutual Key Distribution of Group keys

In the previous sections we discussed distribution of pairwise keys between any two nodes within the transmission range[6] [7] using server node. Some node possess same characteristics on the network depending on the link they produce the dependency of information that each node has. Such type of nodes are grouped together into a single cluster. The wireless network may have any such clusters.

Step 1: A group of K nodes is chosen.

Step 2: A common mutual key mk is chosen.

Step 3:The server now generates K-1 XOR combination of cluster keys for each node.

Step 4:The clients on the same group can use those keys according to the concept discussed in the previous section and communicate with each other without inetrrupting the server node.

Step5: If two nodes of different cluster want to communicate then it need to contacts the server

Step 6: The cluster is managed using some cluster management techniques.

Step 7: If a new node enters the network then it belong to any one of the cluster thus easy for the server to maintain thereby proving dynamic network.

Request messsage(A to S)

(G, n(A), (n(B), n(C), n(D))

Where G - global key identifier,

n(A) - node identifier.

B,C,D - other nodes in the cluster.

Response message: (S to A, B, C, D)

$\{G, n(B) * (j(B), n(C) * j(C), k_{n(B)} * j(B) \oplus k_{n(C)} * j(C)\}$

$\{G, n(A) * j(A), n(B) * j(B), k_{n(A)} * j(A) \oplus k_{n(B)} * j(B)\}$

$\{G, n(C) * j(C), n(D) * j(D), k_{n(C)} * j(C) \oplus k_{n(D)} * j(D)\}$

Upon receiving message [1] the node A does not receive any key, but node B receives node C's local key identifier and node C receives node B's local key identifier. Upon receiving message [2] node A receives node B's local key identifier and node B receives A's local key identifier and C by substituting node B's local key identifier retrieves A's local key identifier. Also node A by substituting B's identifier in message[1] retrieves C's identifier. Now A possess B,C identifiers, B possess A,C identifiers and C possess A,B identifiers. Upon receiving message [3] A,B,C retrieves D's local key identifier. Now A,B,C,D possess all the other nodes local key identifiers using which it has the authentication of the nodes in the cluster and start exchanging messages.

Node Blocking of Compromised Nodes:

Any layer of security has some loop holes [17] to enter. Each node within the wireless transmission range contains the local key identifiers of all the other nodes in the cluster. By capturing of any one node the attacker can revoke C key node identifiers and local key identifiers of the same cluster thereby revoking 2(C+C*) identifiers. Thus the compromised node is isolated from the network. This process is done by the server. The server and the other nodes easily identifies that a node has been neutralized by the message it receives from the compromised node

Step 1: Server sends message to all the nodes to revoke its key identifiers from compromised node.

Step 2: The server deletes all the identifiers of the compromised node from its memory.

Step 3: The client nodes authenticates the alert message from the server and deletes all the identifiers and detaches the link to the compromised node.

Step 4: The client nodes and the server thereby removes the compromised node from the key ring.

III. Performance Evaluation

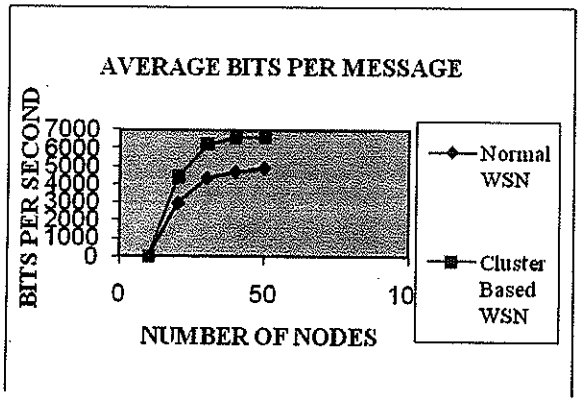


Fig. 3 : Zvaluation Measuring Speed

Our proposed system has proven to be effective because the method is designed by keeping the resource level and complexity in mind. Since the nodes transfer only limited number of keys the speed is increased than the existing mechanisms.

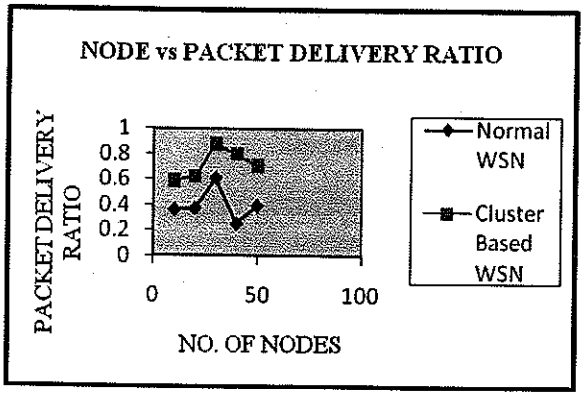


Fig. 4 : Zvaluation Measuring Throughout

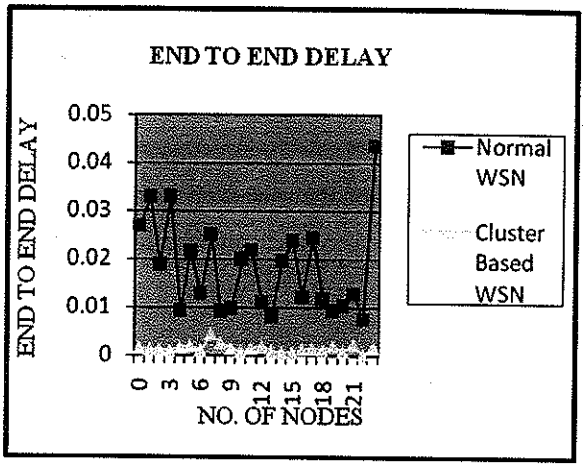


Fig. 5 : Zvaluation Measuring Delay innings

Similarlily the performance is measured with throughput and delay timings. The throughput of existing method is less due to the length of the key used to exchange messages. Also the time for delivery of the message is low because the base station is not subject to single point of attack due to the application of Physically Unclonable Functions (PUF's) and communication overhead on the network.

Performance evaluation [11] is done based on the following attacker models:

- Eavesdropping attack.
- Replay attack
- Syn flooding attack.
- Selective forwarding attack.
- Sinkhole attack.
- Sybil attack.
- Worm hole attack.
- Hello flooding attack.
- Single point of attack.

All the above said attacks are handled with three possible solutions. In the first type of attack the attacker cannot solve the linear system of equations to solve the XOR combination of keys to gain the shared secret key. In the attacks b-h the solution is any node on the network does not accept messages encrypted with and invalid key or irrelevant transfer of messages avoiding other type of attacks. In the attack i, the attacker tries to gain access to the memory of the server and gain table of encrypted keys and identifiers. This is solved by restricting the access to memory of server by using Arbiter based Physically Unclonable Functions [14] [15] (PUF) to protect data.

The existing tampering methods extract secret keys form digital Integrated Circuits such as smartcards, ATM's etc. The PUF reduced the delay between wires and transistors in IC's. The arbiter based PUF's are made up of custom silicon to protect from temperature and power supply voltage.

Some existing tampering methods [20] are:

- Micro probing.
- Laser cutting.
- Glitch attacks.

These attacks remove smart card package and reconstruct the circuit using chemical and optical methods. The solution is to provide additional metallization layers which act as mesh network. Silicon can be used to store pseudo random functions to store actual bits of secret keys restricted to cloning attacks. Finally the performance is evaluated by speed and throughput as shown in fig: 3 and fig: 4. By using pairwise exchange of keys, cluster keys and simple search techniques the number of bits and the number of message / node is increased.

Recursion of Random keys:

Theorem[18]: i) Chances of getting the same random key.

ii) Chances of getting XOR of the last key with the first key form the key list.

iii) Chances of getting XOR of same two keys.

Probability of getting repeated random keys

$$P(k_i = x \mid k_i \oplus R_1, \ldots . k_n \oplus R_4)$$

where $1 \leq i \leq n$

$$P(A) = P(k_i = x) = 1/2^n$$

Probability of getting last key repeated form key list.

$$P\left(k_j = x \mid P(k_1 \oplus k_i, k_2 \oplus k_3 \ldots . k_m \oplus k_1)\right.$$

where $1 \leq i \leq n$

$P(A/B) = 1/2^{n(m-1)}$ (m <- no. of keys in the list)

Probabiltiy of getting XOR of same keys.

$P(k_i = x \mid k_i \oplus k_i)$ where $1 \leq i \leq n$

$P(A/B) = 1/2^{n(m-1)}$

In general $1/2^n$ is the Probability of Vegenere cipher to be reused.

Brute Force Attack Analysis:

Brute force attack tries with all possible combinations of a key. Example if your key is 2 characters long then the possible permutations are 3,844(lower case alphabets = 26 + uppercase alphabets= 26+ numbers 1-10 = 62, 2^{62} =3,844). This takes the general formula n(n-1).....n(k+1). 256 symmetric key is secure against brute

force attack to encrypt the secret key from client node to server node. So implementing RC4 key exchange algorithm with elliptic curve system our network is strong against brute force attack..

Basic requirements:

Each node has C keys in memory. Each client node requires |n| + C *(|j|+|k^{i}) bits of memory. Each server node requires 2$^{|i|}$ *(|i|+|k^{i}|). Random sequence of 64 bits of memory each for 4 nodes is requires. Each node has 8 bits of local key identifiers |j|. Each node also contains 8 bits of node identifiers |n|. Each node also contains a list containing identifiers of communicating nodes. Mobile node stores the nodes of all 4 nodes encrypted with Diffie Hellman key exchange algorithm with Vegenere cipher.

IV Conclusion

The proposed system is a secret key distribution for large sensor networks using limited number of keys. Since newaddition of nodes can be easily carried out it is well suited for dynamic networks. The approach leads to effective distribution of pairwise keys, cluster keys, revoking compromised nodes and authenticating the server which bootstraps the network.

V Scope of Future Work

Even though the system has many advantages, it requires the server node to transmit k-1 XOR combination of keys along with their host name and systems IP address. This is due to linear system of equation in network coding. If random system [21] of equations are used and extended to multi- hop networks our system proves to be still more efficient.

References

[1] P. F. Oliveira, R. A. Costa, and J. Barros, "Mobile secret key distribution with network coding," presented at the Int. Conf. Security Cryptography,Jul. 2007.

[2] P. F. Oliveira and J. Barros, "Network coding protocols for secret key distribution," in Proc. Int. Symp. Information Security, Nov. 2007, pp.1718–1733.

[3] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili,"A pairwise key predistribution scheme for wireless sensor networks,"ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.

[4] D. Malan, M. Welsh, and M. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," presented at the 1st IEEE Int. Conf. Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, Oct. 2004. [Online]. Available: citeseer. ist.psu.edu/ malan04publickey.html.

[5] A. Perrig, R. Szewczyk, J. D. Tygar, V.Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless Netw., vol. 8, no. 5, pp. 521–534, 2002.

[6] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 9th ACMConf. Computer and Communications Security, New York, 2002, pp. 41–47.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. 10th ACM Conf. Computer and Communications Security, New York, 2003, pp. 62–72.

[8] C. Fragouli, J.-Y. L. Boudec, and J. Widmer, "Network coding: An instant primer," Proc. SIGCOMM Comput. Commun. Rev., vol. 36, no. 1, pp. 63–68, 2006.

[9] S. Deb, M. Effros, T. Ho, D. Karger, R. Koetter, D. Lun, M. Medard, and N. Ratnakar, "Network coding for wireless applications: A brief tutorial," presented at the IWWAN, London, U.K., May 2005.

[10] K. Bhattad and K. Narayanan, "Weakly secure network coding," presented at the 1st Workshop on Network Coding, Theory, and Applications, Riva del Garda, Italy, 2005.

[11] F. Stajano and R. J. Anderson, B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, Eds., "The resurrecting duckling: Security issues for ad-hoc wireless networks," in Security Protocols Workshop, 1999, vol. 1796, pp. 172–194, Lecture Notes Comput. Sci., Springer.

[12] F. Stajano, Security for Ubiquitous Computing. New York: Wiley,Feb. 2002. [Online]. Available: http://www.cl.cam.ac.uk/fms27/secubicomp/.

[13] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," J. Amer. Inst. Elect. Eng., vol. XLV, pp. 109–115, 1926.

[14] A. Francillon and C. Castelluccia, "TinyRNG: A cryptographic random number generator for wireless sensors network nodes," presented at the 5th Int. Symp. Modeling and Optimization Mobile, Ad Hoc, and Wireless Networks(WiOpt), 2007.

[15] C. Karlof and D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Netw., vol. 1, no. 2–3, pp. 293–315, 2003.

[16] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. Karger, "Byzantine modification detection in multicast networks using randomized network coding," presented at the IEEE Int. Symp. Information Theory, Chicago, IL, Jul. 2004.

[17] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Trans. Very Large Scale Integr. Syst., vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[18] C. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

[19] B. Schneier, Appl. Cryptography. New York: Wiley, 1994. Oliveira and barros: network coding approach to secret key distribution 423

[20] A. Becher, Z. Benenson, and M. Dornseif, J. A. Clark, R. F. Paige, F. Polack, and P. J. Brooke, Eds., "Tampering with motes: Real-world physical attacks on wireless sensor networks," in Proc. 3rd Int. Conf.

[21] L. Lima, M. Médard, and J. Barros, "Random linear network coding: A free cipher?," presented at the IEEE Int. Symp. Information Theory, Jun. 2007

[22] W. Stallings, Cryptography and network security : principles and practice, Prentice Hall, 1999.] P. van Oorschot A. Menezes and S. Vanstone, *Handbook of Applied Cryptography*,,CRC Press, 1997.

Author's Biography

J.Leka obtained her M.Sc. and M.Phil. Degree in computer science from Bharathiar University. She is working as Assistant professor in Department of Computer Science in Sri Krishna Arts and Science College. She has 5 years of teaching experience. Her area of interest includes network security in wired networks and wireless sensor networks.