ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

Authenticated Channel Aware Encryption For Wireless Sensor Network

S.Velmurugan*, P.M. Rubesh Anand,Diana Aloshius, AarthiAvanthiga

Department of Electronics and Communication Engineering, Hindustan University, Chennai, India

Abstract—Wireless sensor network (WSN) is a collection of sensors organized into a cooperative network. Security and energy consumptionsare considered to be long-lasting technical challenges in WSNs as sensors usually suffer from complexity and energy constraints.In order to avoid the security and energy consumption problems, we propose Channel Aware Encryption along with Key management technique. The core function of exchanging and sharing a secret key between two endpoints is the methodology used in secure key management and it is one of the most critical elements need to be more concerned while integrating cryptographic functions into the system. The proposed work is to apply key pre-distribution schemes for securing and allocating the routes for data transmission from sensor nodes to Ally Fusion Center (AFC). The source node transmits its data to the Ally Fusion Center only through the relay nodes which are having the maximum authentication key value since the key is generated by considering the energy of a node and the distance between two nodes.

Index Terms—Key distribution, Eavesdropping, Encryption, Wireless Sensor Networks.

I. INTRODUCTION

Wireless sensor networks have generated steadily growing interest recently, especially in the field of battlefield surveillance and environment monitoring. number of sensor nodes which are deployed over an area to perform local computations based on information gathered from the surroundings.In practice, sensors for the distributed detection in WSNs are often incapable of employing traditional cryptographic techniques due to practical constraints of sensors such as limited energy resources, and computing power [1]. Hence, there is a possibility that attackers would have chances to disrupt or control the entire network just by monitoring sensor's observations. To resolve the technical challenge of secure communications in WSNs, there have been several notable approaches [2]–[5], where the ability of the physical layer is explored as a solution to the data confidentiality for the distributed detection in WSNs.

Energy is a very scarce resource for such sensor systems and has to be managed wisely in orderto extend the life of the sensor nodes for the duration of a particular mission.One of the major sources of energy loss is idle listening,that is, (listening to an idle channel in order to receive possible traffic) and the other reason forenergy loss is collision (When a node receives more than one packet at the same time, thesepackets are termed collided), even when they coincide only partially. All packets that cause thecollision are discarded and retransmissions of these packets are required which increasesthe energy consumption. The next reason for energy loss is overhearing (a node receivespackets that are destined to other nodes). The fourth one occurs as a result of control-packetoverhead (a minimal number of control packets should be used to make a data transmission).Finally, over-emitting is another reason forenergy loss which is caused by thetransmission of a messagewhen the destination node

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

is not ready.In [2], the signals from the interfering group are used only for confusing the EFC. But in the proposed scheme, the signals of the activated sensors from both the flipping and non-flipping groups are combined at the AFC, and thus the energy consumed by sensors to transmit signals is not wasted, which leads to better energy efficiency.

Our contributions in the work are summarized as follows: Applying key pre-distribution technique (i)To ensure secure data transmission from sensors to Ally Fusion Center (AFC). ii) To utilize energy efficiently during allocation of routes and security key generation in wireless sensor network.

II. RELATED WORKS

In [6], physical layer security for data confidentiality which is tailored to wireless sensors suffering from limited resources in a distributed detection scenario is considered. In particular, for a WSN where sensors report their binary local decisions over a PAC, they displayed that by carefully utilizing a free natural resource, i.e., randomness of wireless channels, it is possible to make the EFC totally ignorant of the target state, i.e., perfect secrecy.Besides the general results of physical-layer security for wireless communications [7]–[8], the proposed scheme is closely related to existing works in three specific areas: (i) secret key extraction from wireless channel [9]-[11], (ii) cooperative secrecy [12]–[13], and (iii) secret communication using artificial noise [14].In [9]-[11], wireless channel gains are considered as common randomness exclusively shared by transmitter and legitimate receiver using the TDD protocol. The works of cooperative secrecy [12]–[13] and artificial interference techniques [14] provide a great deal of insight into the techniques utilized while they are considered in different communication scenarios such as relay networks and point-to-point and multiuser communications. In [15]-[18], they discussed various Key management technique. It is the basis to establish the secure communication using cryptographic technologies between sensor nodes in a sensed area. Huang [19] proposed a structured key-pool random key pre-distribution (SKRKP) scheme to systematically distribute secret keys to each sensor from a structured key pool. Their key pre-distribution scheme includes two steps: key pre-distribution within a given zone and key pre-distribution for two adjacent zones. After the deployment of sensors, each sensor first sets up pairwise keys with all neighbors within its zone; then it sets up a pairwise key with its neighbors located in adjacent zones.Eschenauer and Gligor [20] proposed a random key pre-distribution scheme: before deployment, each sensor node receives a random subset of keys from a large key pool. In order to agree on a key for communication, two nodes find one common key within their subsets and use this key as their shared secret key.

III. PROPOSED WORK

Key management is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed.Key pre-distribution is a mechanism in which keys for each node are chosen from a large key pool. The main goals of a good key pre-distribution algorithm are Key connectivity, Resiliency, Storage requirement and Computational cost and Key Revocation. Key establishment is the process by which right keys for right users can be determined and key rings for each users are sent to them accordingly. Trusted Authority can help in sending the keys to each user through a secure channel. As this mechanism is a costly one and does not suit for sensor networks, we use Key Pre-distribution in which key rings are installed in the nodes before deployment of network in off-line mode.The probability that two sensor nodes in a neighborhood can interact using a pair-wise key is low due to the randomness in the selection of key rings. In such scenarios, senor nodes may take advantage of intermediate nodes to exchange their secret keys so that a direct and secure link can be initiated.

3.1 Random Key Generation:

The wireless sensor network consists of sensor nodes and Ally Fusion Center. Fig. 1 shows that each and every sensor node in the WSN is initially loaded with the randomly generated key by the Ally Fusion Center. The

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

Ally Fusion Center maintains the ID of the nodes present in the network. The key ($K_{randomkey}$) is assigned to the nodes in the list maintained by the Ally Fusion Center only. Each and every node sends the authentication request to its one hop neighbors.

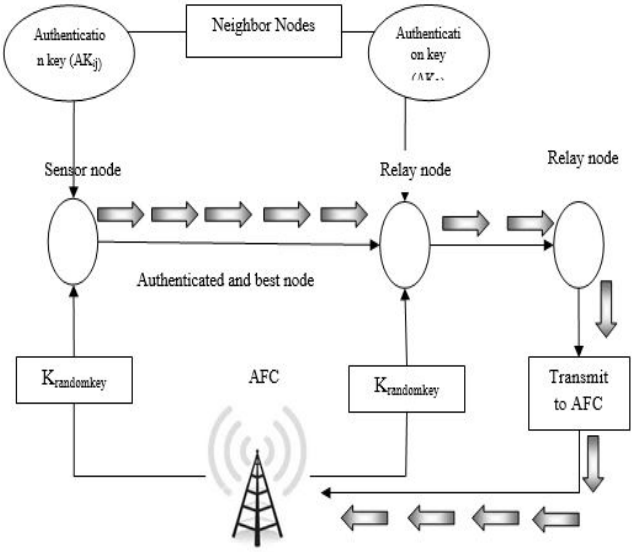

Fig. 1. Architectural Diagram of Authenticated Channel Aware Encryption.

The node checks its privilege by checking its random key. If it has the random key assigned by the Ally Fusion Center,then the node sends the authentication reply as the authentication key. The source node transmits its data to the Ally Fusion Center only through the relay nodes which are having the maximum authentication key value since the key is generated by considering the energy and the distance.

3.2 Authentication using Random Key:

Once the nodes are loaded with the randomly generated key, all the nodes in the wireless sensor network get the authentication key from its neighbor (i.e.,) the node with one hop distance by sending authentication request packet. The authentication request packet contains the node ID, the energy of that node, the distance between that node and its neighbor node. The neighbor node accepts its request and sends the authentication response packet which contains the authentication key along with its ID. The Authentication key is calculated by using the formula,$AK_{ij}=E_j/d_{ij,}$ wherei, jare node IDs. When the source node intends to transmit the data packet, the source node enters into the route discovery phase of Ad hoc On-Demand Distance Vector (AODV) for wireless mesh networks. The source node does as per the following algorithm to select the next authenticated forwarder.

3.3 Algorithm for transmitting data using Authentication Key:

When a source node is ready to transmit the data to the Ally Fusion Center (AFC), it checks the distance whether AFC is near to that node. If yes, it will directly transmit data to AFC. If AFC is out of the range, it transmits data through nearby nodes. For proper delivery of data, following steps should be considered;

Step 1: Get the authentication key from its neighbors.

Step 2: Neighbor nodes send its authentication code along with its randomly assigned key ($K_{randomkey}$).

Step 3: The source node check the nodes privilege by analyzing its $K_{randomkey.}$

Step 4: The source node check the authentication of each of its neighbors.

Step 5: The node which has the maximum value of authentication key is selected as next forwarder due to authentication key as generated by using the residual energy and the distance.

IV. SIMULATION RESULTS AND DISCUSSIONS

In this section, performance evaluations of energy and packet loss ratio are considered. Experimental measurements have shown that generally data transmission is very expensive in terms of energy consumption, while data processing consumes significantly less. The energy cost of transmitting a single bit of information is

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

approximately the same as that needed for processing a thousand operations in a typical sensor node. The energy consumption of the sensing subsystem depends on the specific sensor type. Fig.2 (a) shows that the energy is utilized efficiently in the proposed method (Authenticated Channel Aware Encryption).The packets in the proposed method are transferred from source node to destination node, hence the energy reduce gradually. In our method,21 nodes are implemented in the sensing environmental field and the key pre-distribution scheme where the energy dissipation is less when compared to existing method. Here the energy is compared with reference to time. Fig.2 (b) shows the packet loss ratio, in which the packet loss is less in the proposed method compared to the existing method.

(a)

(b)

Fig. 2(a) Energy and (b) Packet loss Ratio Comparison between Channel Aware Encryption (RED) and Authenticated Channel Aware Encryption (GREEN).

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

(a)

(b)

Fig.3 (a) Packet delivery ratio and (b) Packet delay Comparison between Channel Aware Encryption (RED) and Authenticated Channel Aware Encryption (GREEN).

Fig.3 (a) shows the number of data messages received by the base station over time of operation. The aggregated data is send to the base station by authentication key. Hence the data messages send to AFC is more when compared to the existing method. Fig. 3 (b) shows that the packet delay from Source to Ally Fusion Center (AFC) is less when it is compared with existing method. In the proposed method, key pre-distribution method is implemented which shows that delay is reduced.

V. CONCLUSION

Authentication mechanism in wireless sensor network plays a major role in offering data security, data integrity, and data confidentiality services. In most traditional wireless sensor networks, data transmission and reception between nodes results in packet loss and consumption of more energy which in turn reduce the efficiency of whole network. Our work eliminates the chances of such losses to an extent. In this research, we have implemented 21 nodes and AODV protocol which provides less energy dissipation and packet loss. The authenticated Channel Aware method provide high efficiency over life time of the network.

REFERENCES

[1] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," IEEE Communications Surveys & Tutorials, vol. 11, no. 2, Second Quarter 2009.
[2] H. Jeon, D. Hwang, J. Choi, H. Lee, and J. Ha, "Secure type-based multiple access," IEEE Transactions Information on Forensics and Security, vol. 6, no. 3, pp. 763–774, Sep. 2011.
[3] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 3, no. 2, pp. 273–289, June 2008.
[4] V. Nadendla, "Secure Distributed Detection in Wireless Sensor Networks via Encryption of Sensor Decision,"M.S. thesis, Louisiana State University and Agricultural and Mechanical College, Baton Rouge,LA, USA, 2009.
[5] M. Ilyas and I. Mahgoub, "Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems," CRC Press, New York, 2005.
[6] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 8, no. 4, pp. 619–625, April. 2013.
[7] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2470–2492, June 2008.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

[8] M. Bloch and J. Barros, "Physical-Layer Security: From Information Theory to Security Engineering. Cambridge," U.K.: Cambridge Univ. Press, 2011.
[9] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting Channel Diversity in Secret Key Generation from Multipath Fading Randomness," IEEE Transactions On Information Forensics And Security, Vol. 7, No. 5, October 2012.
[10] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," IEEE Transactions on Information Forensics And Security, Vol. 5, No. 2, June 2010.
[11] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," IEEE Communication Letters, vol. 4, no. 2, pp. 52–55, Feb. 2000.
[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Transactions on Signal Processing, vol. 58, no. 3, pp. 1875–1888, March 2010.
[13] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," IEEE Transactions on Information Theory, vol. 57, no. 1, pp. 137–155, June. 2011.
[14] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," IEEE Communication Letters, vol. 14, no. 10, pp. 885–887, October 2010.
[15] A.Rasheed and R. N. Mahapatra, "Key Pre-distribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks" IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 1, pp, 176-184, January 2011.
[16] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks," ACM Transactions on Information and System Security, Vol. 8, No.1, pp. 41-77, February 2005.
[17] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks,"IEEE Symposium on Research in Security and Privacy, pp. 197-213, May 2003.
[18] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, " A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge," IEEE Trans. on Dependable and Secure Computing. Vol. 3, pp: 62-77, 2006.
[19]D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key management scheme for wireless sensor networks," Proc. 2nd ACM Sorkshop on Security of Ad hoc and Sensor Networks, pp. 29–42, 2004.
[20] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," Proceedings of the ACM conference on Computer and communications security, Washington, DC, USA, pp. 41–47 November 2002.