Virtual Energy Based Encryption Keying framework for WSN: A Survey

Sukhjinder Kaur[1], Abhilasha [2]
Student[1,] Associate Professor[2], GZS PTU Campus Bathinda
kular.sukhjinder666@gmail.com

Abstract

A wireless sensor network consists of sensor nodes which are resource limited wireless devices and it is difficult to recharge them due to hostile environment. Energy consumption and security are the main concerning factors during transmission in wireless sensor networks. Therefore it is required to consume minimum energy without risking security of wireless networks. Less energy consumption prolongs the life time of the sensor nodes. VEBEK is a secure and energy efficient communication framework which is based on dynamic key generation mechanism using RC4 algorithm and it is able to detect and filter false data injected into the network by malicious outsiders. VEBEK consists two operational modes- VEBEK-I & VEBEK-II. In this paper both the modes of VEBEK has explained.

Index terms- *WSN, Security, Energy efficient, RC4 Encryption, Virtual Energy*.

Introduction

The Wireless Sensor Networks (WSN) is playing a very dominant role in various applications including environmental, military, commercial enterprises and industries on geographic area. In another aspects, the underwater sensors nodes are very useful in the oceanographic data collection, pollution monitoring, navigation, military and naval surveillance and mining operations. WSN consists of independent small-sized Sensor nodes. Each sensor node receives data, processes it and sends the information to different destinations. However, unlike wired network with large bandwidth capacity and processing power, WSN has some unique features like Sensor devices are energy limited, computation, and communication capabilities; Figure 1 shows the general model for WSN [3] as Sensor nodes are usually deployed in large numbers usually in unattended environment which makes it vulnerable to physical attack; WSN is used to monitor physical environments and unattended nature and wireless media increases the likelihood of various attacks. Protocols should be resilient against false data injected into the network by malicious nodes.

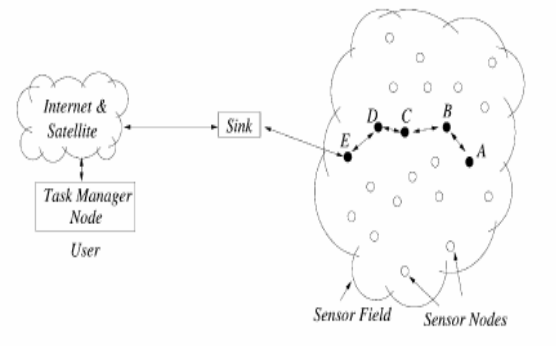

Figure 1Sensor nodes scattered in WSN

Keying mechanism for security in WSN has been discussed. There are two types of keying mechanisms for WSNs: *static and dynamic*. In static key management Schemes, either fixed number of keys are preloaded on the sensor nodes at the time of deployment of the node or shortly after deployment. In this management, key generation and distribution are handled statically. On the other hand dynamic key management schemes perform rekeying either periodically or on demand as needed by the network. The sensor nodes exchange keys dynamically for the communication.

1. A dynamic key generation scheme that does not require exchanging extra messages;
2. One-time dynamic keys for each packet transmission to avoid stale keys;
3. Modular and flexible security architecture with a simple technique for ensuring

authenticity, integrity, and non-repudiation of data without enlarging packets with MACs;
Dynamic key management is more attack resilient but it increases the communication overhead due to keys being refreshing or redistributed time to time in the network. Due to the overhead incurred in key management, more energy of network is consumed.
In Wireless Sensor Network (WSN), VEBEK is a secure communication framework which is based on dynamic key generation mechanism. VEBEK dynamically update keys without exchanging messages and without appending message authentication codes (MAC). Keys are generated using RC4 encryption scheme which is based on permutation code generation method. RC4 scheme is secure encryption scheme. RC4 algorithm is used for encryption and decryption. Key to the encryption scheme dynamically changes as the residual virtual energy of the sensor, therefore no need for rekeying. This protocol is applicable in highly error prone area like under water operations.

Related Work

During transmission of data packets from source to destination, dynamic filtering of malicious packets has been the focus of several studies, including statistical en-route filtering (SEF) [9], Lightweight Security Protocol (LISP) [10], Security Protocols for Sensor Networks (SPINS) [11] and Location-Aware End-to-End Data Security (LED) [12] ,where they were compared with the VEBEK framework,
Fan Ye Haiyun Luo and Songwu Lu [9] proposed the "Statistical En-route filtering of injected false data in sensor networks" mechanism to detect the reports during the forwarding process and drop them if the injected data in reports is false. It may possible that same event can be detected by multiple sensors, in SEF each of the detecting sensors generates a keyed message authentication code (MAC) and multiple MACs are attached to the event report. When the report is forwarded, each node along the way verifies the correctness of the MAC's probabilistically and drops those with invalid MACs. Multiple detections are done by multiple sensor nodes before accepting the data.

Taejoon Park and Kang G. Shin [10] proposed the "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks" which is based on efficient rekeying technique used for both small and large networks. LISP include efficient key broadcast without retransmission or ACK. It is having ability to detect and recover lost keys and key refreshment without disrupting ongoing data encryption/ decryption. LISP decompose entire network into clusters or sensing groups and additionally it uses intrusion detection system (IDS) to find malicious activities within the network.
A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. Tygar [11], proposed the "SPINS:-Security Protocols for Sensor Networks", which is basically concern with security issues. It has two secure building blocks: SNEP and _TESLA. SNEP provide data authentication, data confidentiality and data freshness between two parties and _TESLA provide broadcasting. Both reduce communication overhead by reusing the code.
Kui Ren and Wenjing Lou and Yanchao Zhang [12] proposed the "LEDS: Providing Location-Aware End-to-End Data Security", in Wireless Sensor Networks which is also a key management framework where each key is blind with location information. Basically three types of keys are used in this mechanism; a) two unique keys are shared between nodes and sink to provide authentication between them, b) call key shared with other nodes for data confidentiality, c) set of authentication keys shared with nodes and reporting path nodes to provide cell to cell authentication. But there are some disadvantages of LED as it requires many keys for communication and it is not possible to change cell dynamics after key generation

VEBEK framework modules

VEBEK frame work having basically three modules named Virtual energy based keying module, Crypto module and forwarding module. A high-level view of the VEBEK framework and its underlying modules are shown in Fig. 1

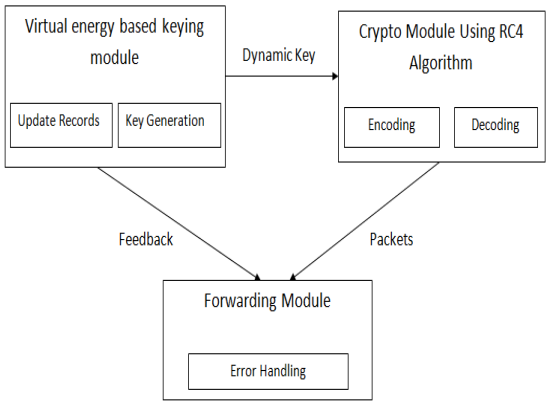

Fig 2: Modular Structure of VEEEK

A. Virtual Energy-based Keying module

Virtual energy based keying module involves the process of creation of dynamic keys. It generates a new unique key as the data is sensed and ensures that each packet is having a different key. Generated dynamic key is then fed into the crypto module. Each node then computes and updates the transient value of virtual energy on the basis of actions that have performed. Each action on node is associated with some predefined cost. The set of actions and their associated energies for VEBEK includes packet reception, packet transmission, packet encoding, packet decoding energies and energy required to keep a node alive in the idle state. The transient value of the virtual energy is calculated by decrementing the total these predefined associated costs from the previous virtual energy. This module is totally based on the watching concept.

B. Crypto Module

The module performs the simple encoding operation using RC4 encryption mechanism based on permutation. The key generated by virtual energy based keying module is used as input for RC4 algorithm. The purpose of crypto module is to provide confidentiality of the packet data while ensuring the authenticity and integrity of sensed data without incurring transmission overhead of traditional schemes. The packets in VEBEK consist of the ID, type and data fields and each node sends these to its next hop. RC4 encryption algorithm takes the key and the packet fields as inputs and produces the result as a permutation code. The concatenation of each 8-bit output becomes the resultant permutation code. This simple encoding is beneficiary as: 1) there is no hash code is used in transmission; the packet size does not increased, network lifetime increases 2) this simple technique is ideal for resource limited devices 3) no need of control messages for rekeying in RC4.

C. Forwarding Module

The final module in VEBEK communication framework is forwarding module. The forwarding module sends packets from the current node or received packets from the other nodes along the path to sink and the whole procedure is done by using two algorithms: Source Node Algorithm and Forwarder Node Algorithm.

I. Operational modes of VEBEK framework

The VEBEK protocol is secure framework which provides three security services: Integrity, Authentication and nonrepudation. The main reason behind providing these services is the watching mechanism [1]. The VEBEK framework basically consists of two operational modes have shown in Fig. 2and details of both given below.

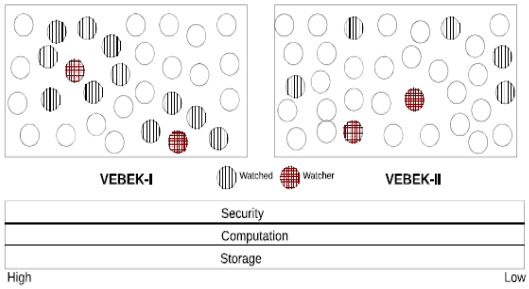

Fig. 3. Operational modes of VEBEK

A. VEBEK-I

In VEBEK-I operational mode, all nodes watch their neighbor nodes. Whenever the packet is received from its neighbor node, it is decoded and its integrity and authenticity are verified. If the packet is legitimate then it is forwarded toward the sink otherwise dropped. In this

operational mode, a small window of time is assumed at the time of deployment of nodes during which an attacker can capture a node or get keys. During this small period of time, each node can decide which node to watch and a record r is stored for each of its one hop neighbors in its watch list. When an event occurs and a record is generated, it is encoded as a function of the dynamic key based on virtual energy of the current node and transmitted. When the packet arrives at the next node, key is extracted from the record of sending node. At the receiving node, if packet is decoded successfully, it is compared with the plaintext ID. In this process, if the forwarding node is not able to extract the key successfully it will decrement the predefined virtual energy value from the current perceived energy and tries for another key before declaring the packet as malicious. The process repeated for several times. If the packet is authentic and this node is node the destination node then packet is re-encoded with its own key and forward to the next node otherwise discarded. The whole process continues until packet reaches the destination node (sink).

B. VEBEK-II

In the VEBEK-II operational mode, only few nodes are watched by the nodes in the network. Each node randomly picks r nodes to watch and store corresponding state before deployment. As the packet leaves the source node it passes through the watching node. VEBEK-II is a statistical filtering approach. If the current node is not watching the node that had sent the packet, the packet is just forwarded without checking. If the current node is watching the node that generated the packet then the packet will be decoded and compared with plaintext ID. If the forwarder-watcher node cannot find the key successfully then it will try for many keys before declaring it malicious as done in previous mode. If the packet is authentic, and this hop is not the final destination, the original packet is forwarded unless the node is currently bridging the network. In the bridging case, the original packet is re-encoded with the virtual bridge energy and forwarded. Since this node is bridging the network, both virtual and perceived energy values are decremented accordingly. If the packet is illegitimate, which is classified as such after exhausting all the virtual perceived energy values within the virtual Key Search Threshold window, the packet is discarded. This process continues until the packet reaches the sink.

Benefits and Limitations of VEBEK

This section briefly summarizes several benefits and limitations of the VEBEK secure communication framework. The VEBEK framework has the following benefits:

• *No control messages for rekeying:* VEBEK does not exchange control messages for key renewals as opposed to other dynamic key management schemes. Therefore, VEBEK is able to save more energy and is less chatty in nature.

• *One-time key:* In VEBEK, one key per message is employed. For the successive packets of the stream, different keys are used while the other schemes use basically the same key for different packets. This dynamic nature also makes the VEBEK framework more resilient to certain attacks (e.g., replay attacks, brute-force attacks, and masquerade attacks).

• *Modular architecture:* Since keys are generated in a separate module in VEBEK, other key-based encryption or hashing schemes can also be adopted easily.

• *Reduces transmission overhead:* VEBEK-I reduces transmission overhead as it is able to catch malicious packets in early stages. Due to this method Less energy consumed.

There are some limitations also of this framework as;

• VEBEK–I increases processing overhead as decoding and encoding is done at every node.

• VEBEK-II has more transmission overhead because packets from malicious node may or may not be caught by the intermediate nodes and may reach the sink.

Conclusion

Communication is very costly for wireless sensor networks and certain applications. It is very important to minimize the exchange of the messages as it is essential in e.g. military

scenarios. A secure communication framework for WSN is VEBEK as it based on the idea of using dynamic keying mechanism for communication between nodes. We have analyzed that VEBEK is feasible and secure framework. We have discussed that different operational modes of VEBEK (VEBEK-I & VEBEK-II) having optimal ability to perform better in variety of network configurations.

References

[1] Arif Selcuk Uluagac, Raheem A. Beyah, Yingshu Li and John A. Copeland, "*VEBEK: Virtual Energy Based Encryption and Keying for wireless Sensor Networks*," Vol. 9, No. 7, JULY 2010.

[2] K. Ravi Chythanya, S.P.Anandaraj.and S. Padmaja, *"Virtual Energy-Efficient Encryption and Keying (VEEEK) for Wireless Sensor Networks*," International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 8 August 2011.

[3] K. Naga Krishnaja, "*Cryptography via Virtual Energy for Wireless Sensor Networks,"* International Journal of Information and Education Technology, Vol. 2, No. 1, February 2012.

[4] Abu Shohel Ahmed, "*An Evaluation of Security Protocols on Wireless Sensor Network,"* TKK T-110.5190 Seminar on Internetworking, April 2009.

[5] S.P. Santosh Kumar, C.B. Sivaparthipan, D. Prabhakar and Dr. S. Karthik, "*Secure Encryption Technique with Keying Based Virtual Energy for Wireless Sensor Networks,"* Vol. 1, Issue 5, October 2013.

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "*Wireless Sensor Networks: A Survey," Computer Networks*, vol. 38, no. 4, pp. 393-422, Mar. 2002.

[7] C. Vu, R. Beyah, and Y. Li, "A Composite Event Detection in Wireless Sensor Networks," Proc. IEEE Int'l Performance, Computing, and Comm. Conf. (IPCCC '07), Apr. 2007.

[8] Adrian Perrig and Robert Szewczyk and J.D. Tygar and Victor Wen and David E. Culler. SPINS: security protocols for sensor networks. In ACM Wireless Networks, volume 8, 2002.

[9] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE JSAC, vol. 23, no. 4, pp. 839-850, April 2005.

[10] Taejoon Park and Kang G. Shin. LiSP: A Lightweight Security Protocol for Wireless Sensor Networks. In ACM Transaction, June 2004.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. Tygar, "Spins: Security Protocols for Sensor Networks," Proc. ACM MobiCom, 2001.

[12] Kui Ren andWenjing Lou and Yanchao Zhang. LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. In Mobile Computing, IEEE Transactions, volume Voloume: 7, Issue: 5, page 585, May 2008