ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

VEBEK-III: A Modified Technique of VEBEK to Save Energy in WSN

Sukhjinder Kaur[1], Abhilasha[2]
[1] Student, [2] Associate Professor, GZS PTU Campus Bathinda, India
Sukhjinder_90@yahoo.com

Abstracts

In Wireless Sensor Network (WSN) energy rate of consumption is very important factor because once the energy of node is consumed it can't be regenerated and node becomes dead. It is nearly impossible to replace the dead node due to hostile environment. Each node has some initial energy. Energy of node is consumed during reception, transmission and processing of data packets. Therefore energy of node should be optimally utilized during these tasks. Another important issue in WSN is security of data packets transmitted through the network. Previously VEBEK-I & VEBEK-II are two techniques proposed to consider the network security. But these protocols consume a lot of energy during security checks. In this paper, a flag based technique VEBEK-III has been introduced to reduce energy consumption along with security checks. The results of VEBEK-III outperformed with VEBEK-I and VEBEK-II in case of energy consumption and has more security than VEBEK-II.

Keywords: WSN, Security, Energy efficient, Virtual Energy, VEBEK-I, VEBEK-II, VEBEK-III.

Introduction

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. 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. 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.

In 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.

Semantics of VEBEK

The VEBEK framework is comprised of three modules: Dynamic Key generation, Cryptography, and Forwarding [5]. The virtual energy-based keying process involves the creation of dynamic keys. Contrary to other dynamic keying schemes, there is no exchange of extra packets to generate key. Dynamic key is generated on the basis of residual virtual energy on sensor node at that particular time. The key is then sent to cryptography module. The cryptography module does encoding on packet and use the dynamic key to encode packet. RC4 algorithm has used for encryption. VEBEK's flexible architecture allows for adoption of stronger encryption mechanisms in lieu of encoding [7]. Lastly, the forwarding module handles the process of sending or receiving of encoded packets along the path to the sink. A graphical view of VEBEK framework and its underlying modules are shown in figure 1.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

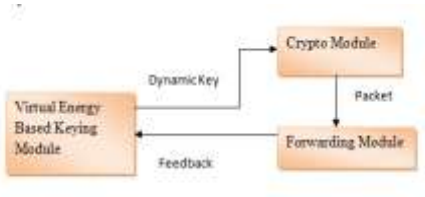

Figure 1: Modular structure of the VEBEK framework.

In VEBEK, the tracking of virtual residual energy of sending node at the receiving node is called watching. Watching concept is illustrated with an example in figure 2.

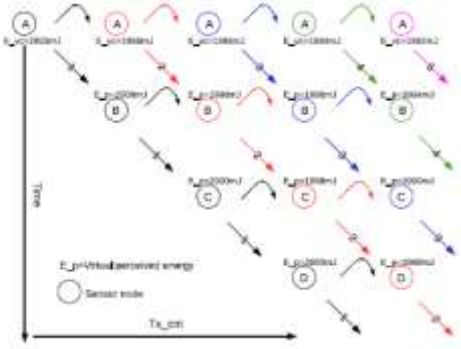

Figure 2 An illustration of watching concept with forwarding

In the figure, there is one source sensor node, A, and other nodes B, C, and D are located along the path to the sink. Every node watches its downstream node, i.e., B watches A (B < A); C watches B (C < B); D watches C (D < C). All the nodes have the initial virtual energy of 2000mJ and as packets are inserted into the network from the source node (A) over time, nodes decrement their virtual energy values. Node A starts with energy 2000mJ as the first key to encode the packet and node A sends the packet to the next node by decreasing its virtual energy to 1998mJ. Node B receives the packet and decode it using perceived energy value (E_p=2000mJ) and update E_p after sending the packet. The virtual energy becomes Shared dynamic cryptic credential after reaching sink.

Operational Modes of VEBEK

The VEBEK protocol provides three security services: Authentication, integrity, and non-repudiation. The fundamental notion behind providing these services is the watching mechanism described before. The watching mechanism requires nodes to store one or more records to be able to compute the dynamic keys used by the source sensor nodes, so that they can decode packets, and to detect unauthenticated packets either due to communication problems or potential attacks.. In reality, applications may have different security requirements. For example, need of the security in military application of Wireless Sensor Network (e.g., doing survey of portion of a combat zone) may be higher than that of a civilian application (e.g., collecting temperature data from a national park).

There is a need of flexible frame work. Due to this need there are two operational modes in VEBEKVEBEK-I and VEBEK-II. These modes are based on number of sensor nodes they watch for authentication check of packet. VEBEK-I considers packets coming from all neighbors for authentication check while VEBEK II will check packets coming from particular neighboring nodes.

VEBEK-I

In the VEBEK-I operational mode, all nodes check for authentication of packet coming from their neighbors; whenever a packet is received from a neighbor sensor node, it is decoded and its authenticity and integrity are verified. Only authenticated packets are sent to the destination. In this mode, there is a short window of time assumed at initial deployment that an adversary is not able to attack the network, because it is very difficult to catch a node of keys which are based on residual virtual energy. During this period of time, information of initialization of route may be used by each node to decide which nodes are its neighbor nodes. To obtain a neighbor's initial energy value, a master key can be used to transmit this value during this period similar to the shared-key discovery phase of other dynamic key management schemes. Alternatively, sensors can be pre-loaded with the initial energy value.

When an event occurs and a report is generated, it is encoded as a function of a dynamic key based on the virtual energy of the originating node, and transmitted. When the packet arrives at the next node, the receiver node gets the key of sender node from the record (the virtual perceived energy value associated with the sending node and decodes the packet). Then packet is decrypted and after the successful decryption of packet the authentication of packet is checked. To do this authentication check, the plaintext ID is compared with the decoded ID. If the receiving node is not able to successfully extract the key then it will decrease the predefined virtual energy value from the current perceived energy and tries another key before classifying the packet as malicious (because dropping of packet may have occurred many times due to communication errors). This process is repeated several times; and total number of trials of unsuccessful decryption of packet is needed to classify. Then this value is compared with Virtual Key Search Threshold. If this value (value of count of unsuccessful trials) is less

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

than threshold value then packet is consider as authentic, and if this node is not destination node then the packet is encoded again and forward to next node. But if value of unsuccessful count is more than threshold value then packet is considered as unauthenticated and it is dropped. This process will stop when the packet will reach its destination.

Re-encoding of packet at every hop will increase the strength of the encryption. The general packet structure is [ID, {ID, data}]. Here ID is the ID packet of packet and {ID, data} is encrypted at each node using dynamic key for their encryption. VEBEK-I reduces the transmission overhead as it will be able to catch malicious packets in the next node, but processing overhead increases in VEBEK-I because of the encryption/decryption occurs at every node.

VEBEK-II

In the VEBEK-II operational mode, wireless sensor nodes check authentication of packet coming from some specific neighbor nodes. Each node picks some m nodes randomly and monitors only those m nodes. Then packet is encrypted at source node and forward to the next node. If the receiving node is not watching the node (from which packet has arrived) then that packet will be forwarded without authentication check. If the node from which the packet is coming is in watch list of receiving node than decoding, authentication check, encoding and forwarding is done on that packet on that node. Similar to VEBEK-I, if the receiver node is not able of successfully extract key of packet than value of unsuccessful check is compared with virtual Key Search Threshold before actually dropping the packet as malicious. If the packet is legitimate, and current node is not the destination node than packet is forwarded to the next node.

If the packet is classified as unauthenticated, after value of unsuccessful search exceed Virtual Key Search Threshold than such packet is discarded. This process is repeated until the packet doesn't reach destination. Transmission over head is more in this mode because illegitimate packet can remain unchecked and can reach to destination. But processing overhead will be less in this mode as compared to VEBEK-I because packet will not be encrypted/decrypted at each node. Also the energy consumption of this mode is less than VEBEK-I. There is a tradeoff of energy and security in both operational mode of VEBEK.

VEBEK-III

The proposed algorithm mainly focuses to reduce the energy consumption in VEBEK. To reduce energy consumption flag values has been used at nodes. If value of flag will be 1 then authentication check will be performed otherwise packet will be forwarded without checking. It will do security check at every node having 1flag value and it will also prolong the life of network. The algorithm to do this is as follow.

Algorithm Forwarding Module with flag values

1. Create packets of file.
2. Find shortest path
3. Repeat for each packet
4. If (node.flag==0)
5. If(node==source)
    a. Generate dynamic key.
    b. Encode and forward packet to next node
    c. Reduce encoding and forwarding energy.
6. Otherwise, If (node ==destination)
    a. Decode packet and check for its authentication
    b. Reduce receiving and decoding energy.
7. Otherwise,
    a. Forward packet to next node.
    b. Reduce forwarding energy from node.
8. Otherwise,
9. If(node==source)
    a. Generate dynamic key.
    b. Encode and forward packet to next node.
    c. Reduce encoding and forwarding energy.
10. Otherwise, If (node ==destination)
    a. Decode packet and check for its authentication
    b. Reduce receiving and decoding energy.
11. Otherwise,
    a. Decode packet and check for its authentication.
    b. Generate dynamic key.
    c. Encode and forward packet to next node.
    d. Reduce receiving, decoding energy, encoding and forwarding energy.
12. End loop.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Results and discussions

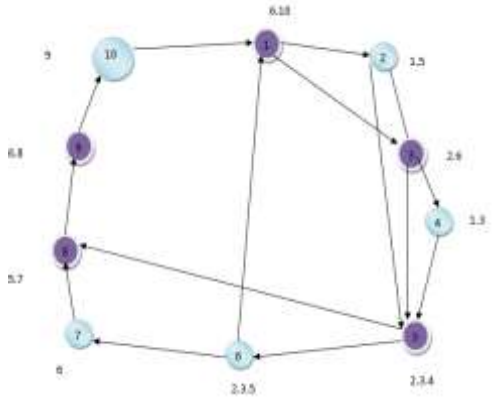

Figure 3 Graph for 10 inputs

The input graph taken to check nodes consists of 10 nodes. This graph is shown in Figure 3 Then the shortest path is 1->3->5->8->9. There has been considered node 1 as source and node 9 as destination. Shortest path form node 1 to node 9 is 1->3->5->8->9. In this path node 3, 5 and node 8 are intermediate nodes. For VEBEK-II it have considered node 3 has node 2 & 6 in its watch list i.e. node number 3 will do authentication check for all packets coming from node 2 & 6 but node 3 doesn't have node 1 in its watch list which means node 3 will not check for authenticity for packets coming from node 1. So in this experiment node 5 will do authentication check for each packet and node 3 will simple forward packets to next node. Residual energy at node 3 after passing each packet is shown in Table1

	VEBEKI	VEBEKII	VEBEK-III
P1	1957	1992	1957
P2	1914	1984	1949
P3	1871	1976	1906
P4	1828	1968	1898
P5	1785	1960	1855
P6	1742	1952	1847
P7	1699	1944	1804
P8	1656	1936	1796
P9	1613	1928	1753
P10	1570	1920	1745

Table 1: Residual Energy at node 3

For node 3 the energies left after sending of each packet in VEBEK-I, VEBEK-II and proposed method VEBEK-III is shown in Figure 5. VEBEK-II has more energy and VEBEK-I have less energy presented than VEBEK-III at node 3 after transference of each packet.

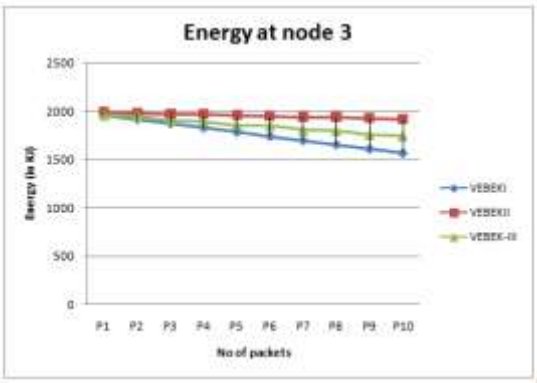

Figure 4: Energies left at node 3 after sending each packet.

Residual energy at node 5 after passing each packet is shown in Table 2.

	VEBEKI	VEBEKII	VEBEK-III
P1	1957	1957	1992
P2	1914	1914	1949
P3	1871	1871	1941
P4	1828	1828	1898
P5	1785	1785	1890
P6	1742	1742	1847
P7	1699	1699	1839
P8	1656	1656	1796
P9	1613	1613	1788
P10	1570	1570	1745

Table 2: Residual Energy at node 5

For node 5 the energies left after sending of each packet in VEBEK-I, VEBEK-II and VEBEK-III is shown in Figure 5.

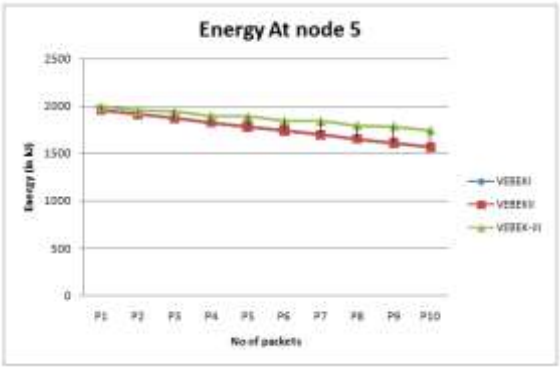

Figure 5: Energies left at node 5 after sending each packet.

In case of malicious attacks, in VEBEK-I unauthenticated packet is detected at same node, in VEBEK II unauthenticated packets is detected at node which is checking packet coming from its neighbor. And in our proposed technique VEBEK-III unauthenticated

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

packet will be detected at nodes which have flag value 1. It means this can't be told that at which node unauthenticated packet will be detected in VEBEK-II and VEBEK-III. In case of VEBEK-II unauthenticated packet can reach to destination without being checked but it is not possible in VEBEK-III because a check is provided that if all nodes in path have 0 flag value then it should change values of some flags to 1. Therefore in terms of security VEBEK-III is better than VEBEK-II.
In terms of security, when attacker is attacking at node 3 VEBEK-I, VEBEK-II & VEBEK-III detect the malicious packet at different locations. The results are shown using table 3.

	VEBEK-I	VEBEK-II	VEBEK-III
P1	3	5	3
P2	3	5	5
P3	3	5	3
P4	3	5	5
P5	3	5	3
P6	3	5	5
P7	3	5	3
P8	3	5	5
P9	3	5	3
P10	3	5	5

Table 3: Attack detecting node for each packet

Malicious packet detection when attacker attacks at node 3 in three different techniques is shown in figure 6

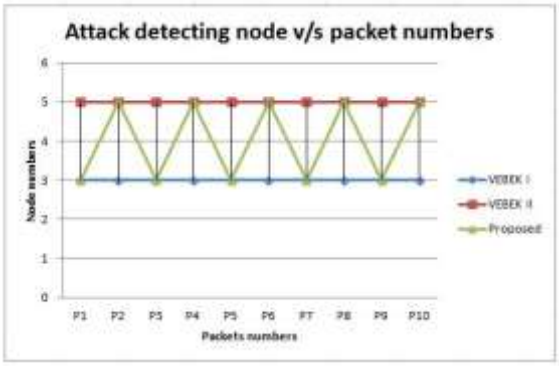

Figure 6: Detection of malicious packet at different nodes

Conclusion and future scope

In this paper, a deep study about wireless sensor network has done. And a new methodology VEBEK-III is proposed which checks for authentication only on nodes if flag value of node is 1 and forwards rest of the packets. The energy is consumed less as compared to VEBEK I. And with comparison VEBEK II in VEBEK-III energy consumption is divided over every node because in each node half packets are checked. But in VEBEK II energy will be reduced for each packet for nodes having previous node of path in their watch list. This have also concluded that VEBEK-III provides better security against unauthenticated packets then VEBEK-II. Hence, it is shown in comparisons that VEBEK-III is better than previous techniques in case where security is not much required.

In future security of VEBEK-II & VEBEK-III can be increased equal to VEBEK-I, and more techniques can be proposed to save energy in VEBEK.

References

1. Z. Yu and Y. Guan (2006), "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," *Proc. of IEEE INFOCOM*, pp. 1–12.
2. F. Ye, H. Luo, S. Lu, and L. Zhang (2005), "Statistical en-route filtering of injected false data in sensor networks*," IEEE JSAC*, vol. 23, no. 4, pp. 839–850.
3. C. Kraub, M. Schneider, K. Bayarou, and C. Eckert (2007), "Stef: A secure ticket-based en-route filtering scheme for wireless sensor networks," *The 2nd Int. Conf. on Availability, Reliability and Security (ARES)*, pp. 310–317.
4. S.P. Santosh Kumar and C.B. Sivaparthipan et.al(2013), " Secure Encryption Technique with Keying Based Virtual Energy for Wireless Sensor Networks", *International Journal of Advance Research in Computer Science and Management Studies*,vol.1 no 5, pp. 139-144.
5. A. S. Uluagac, R. Beyah, and J. Copeland (2010), "VEBEK: Virtual energy-based encryption and keying (vebek) for wireless sensor networks," IEEE transactions on mobile computing, VOL. 9, NO. 7 pp. 994-1007.
6. S. Uluagac, C. Lee, R. Beyah, and J. Copeland (2008), "Designing secure protocols for wireless sensor networks," Lecture Notes in Computer Science, Wireless Algorithms, Systems, and Applications (WASA)., vol. 5258, pp. 503–514.
7. M. Eltoweissy, M. Moharrum, and R. Mukkamala (2006), "Dynamic key management in sensor networks," IEEE Communications Magazine, vol. 44, no. 4, pp. 122–130.
8. Anurag Pandey, Saurabh Srivastava(2013), "Virtual Energy Based Encryption & Keying on Wireless

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Sensor Network" in IOSR Journal of Computer Engineering (IOSR-JCE) Vol 9, No 3 pp 34-43.

9. Dr.S.Bhargavi(2011), "Implementation Of Node Energy Based On Encryption Keying", in . (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 8.
10. H. Hou, C. Corbett, Y. Li, and R. Beyah (2007), "Dynamic energy-based encoding and filtering in sensor networks," in Proc. of the IEEE MILCOM.
11. R. Roman, C. Alcaraz, and J. Lopez (2007), "A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes," Mobile Networks and Applications, Springer, vol. 12, no. 4, pp. 231–244.
12. W. Stallings (2003), Cryptography and Network Security: Principles and Practices (3rdedition). Prentice Hall.