ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Achieving Efficient Security and less Energy Consumption using Node Energy in WSN

Nikhilkumar B S
Asst.Professor Department of Computer Engineering, JSPM's JSCOE Hadapsar, Pune, India

Abstracts

Wireless Sensor Networks (WSN), an element of pervasive computing, are presently being used on a large scale to monitor real-time environmental status Designing cost-efficient, secure network protocols for Wireless Sensor Networks (WSNs) is a challenging problem because sensors are resource-limited wireless devices. Sensor devices are the power consumption devices to achieve low power consumption and high security we need to avoid the rekeying ,stale keys, reducing the false data from malicious node and dynamic energy based keying technology were used. Since the communication cost is the most dominant factor in a sensor's energy consumption, we introduce an Efficient Node Energy Based Encoding (ENEBE) and Filtering of False data Injection. ENEBE and FFDI is able to efficiently detect and filter false data injected into the network by malicious from outside. The Efficient Node Energy Based Encoding (ENEBE) and Filtering of False data Injection (FFDI) consists of two operational modes (OM-I and OM-II), each of which is optimal for different scenarios. In OM-I, each node monitors its one-hop neighbors where OM-II statistically monitors downstream nodes. Our designed framework performs better than other comparable schemes in the literature with an overall percent improvement in energy savings.

Keywords: WSN, Malicious Node, authenticity, integrity, confidentiality. (ENEBE) and (FFDI)

Introduction

Sensor network technology has rapidly developed and will be used in a variety of environments. WSNs consist of a large number of small sensor nodes having limited computation capacity, restricted memory space, limited power resource, and short-range radio communication device. In military applications, sensor nodes may be deployed in hostile environments such as battlefields to monitor the activities of enemy forces.

Securing sensor networks poses unique challenges because these types of networks are usually unattended and have limited energy, computation, and communication capabilities. Protocols are designed such a way that, they must provide greatest strength towards the false data injection by malicious node. The sensor networks must provide the authenticity and integrity between the sources and sink to achieve high security. Dynamic energy based keying technology were used, to achieve low power consumption it avoids the rekeying the transmission of packets and reporting the false data injection in the network by malicious nodes.

However, in this paper we focusing on energy based keying mechanisms and filtering of false data injected in the network for WSN's. There are two fundamental key management schemes for WSNs: static and dynamic. In static key management schemes, key management functions are handled statically dynamic key management schemes perform keying functions either periodically or on demand as needed by the network.

The purpose of this paper is to develop an efficient and secure communication framework for WSN applications. This technique to verify data in line and drop false packets from malicious nodes thus maintaining the health of the sensor network. Each sensed data is protected using a simple encoding scheme based on a permutation code generated with the RC4 encryption scheme and sent toward the sink. The nodes forwarding the data along the path to the sink are able to verify the authenticity and integrity of the data. This framework technique provides high energy efficient compare to other scheme in literature survey with an overall 60-100 per cent improvement.

Related work

Problem Statement

Sending confidential information from one node (source) to another node (destination) on a network could be a challenging task. Using the available resources and energy, the nodes exchange data of the received and sent packets and also ensure data integrity before it hits the sink.

The data exchanged could be manipulated or changed by the hacker on the network. So, the task would be to create a secure system that can ensure safety of the data

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

using encryption methods (such as RC4) and still use the available energy and resources without much overhead.

Objective of the Paper

The objective of this paper is to discuss efficient and secure communication frameworks for Network applications by building upon the idea of sharing a dynamic cryptic credential.

Designing cost-efficient, secure network protocols for any Networks is a challenging problem because all the networks are resource-limited. Since the communication cost is the most dominant factor in a energy consumption, it is necessary to introduce an energy-efficient **Efficient Node Energy Based Encoding (ENEBE) and Filtering of False data Injection** scheme for LAN network that significantly reduces the number of transmissions needed for rekeying to avoid stale keys.

Existing System

In an existing system The Dynamic En-route Filtering (DEF) scheme involves the usage of authentication keys and secret keys to disseminate the authentication keys; hence, it uses many keys and is complicated for resource-limited sensors. In the scheme], a legitimate report is endorsed by multiple sensing nodes using their own authentication keys. Before deployment, each node is preloaded with a seed authentication key and l+1 secret keys randomly chosen from a global key pool. Before sending reports, the cluster head disseminates the authentication keys to forwarding nodes encrypted with secret keys that will be used for endorsing. The forwarding nodes store the keys if they can decrypt them successfully. Later, cluster heads send authentication keys to validate the reports.

Statistical en-route filtering (SEF) In SEF, each sensing report is validated by multiple keyed. Message authentication codes. Specifically, each node is equipped with some number of keys that are drawn randomly from the global key pool. First, a center of stimulus is selected among the source sensor nodes in the event region. Then, once a report is generated by a source node, a MAC is appended to the report. Next, another upstream node that has the same key as the source can verify the validity of the MAC and filters the packet if the MAC is invalid. However, the downside of SEF is that the nodes must store keys and packets are enlarged by MACs.

Secure Ticket-Based En-route Filtering (STEF) by Krauss et al., proposes using a ticket concept, where tickets are issued by the sink and packets are only forwarded if they contain a valid ticket. If a packet does not contain a valid ticket, it is immediately filtered out. STEF is similar in nature to SEF and DEF. The packets contain a MAC and cluster heads share keys with their immediate source sensor nodes in their vicinity and with the sink. The downside of STEF is its one way communication in the downstream for the ticket traversal to the cluster head.

Disadvantages

- Current schemes involve the usage of authentication keys and secret keys to disseminate the authentication keys; hence, it uses many keys and is complicated for resource-limited nodes.
- Current schemes are complicated for resource-constrained sensors as they transmit many keying messages in the network, which increases the energy consumption of WSNs that are already severely limited in the technical capabilities and resources (i.e., power, computational capacities, and memory) available to them.

Proposed System

The ***Efficient Node Energy Based Encoding (ENEBE) and Filtering of False data Injection (FFDI)*** is a secure communication framework where the data is encoded using a scheme based on a permutation code generated via the RC4 encryption mechanism. The key to the RC4 encryption mechanism dynamically changes as a function of the residual energy of the network. Thus, a one-time dynamic key is employed for one packet only and different keys are used for the successive packets of the stream.

The intermediate nodes along the path to the sink are able to verify the authenticity and integrity of the incoming packets using a predicted value of the key generated by the sender's virtual energy, thus requiring no need for specific rekeying messages.

ENEBE and FFDI's flexible architecture allows for adoption of stronger encryption mechanisms in lieu of encoding. And also show that our framework performs better than other comparable schemes in the literature with an overall 60-100 percent improvement in energy savings without the assumption of a reliable medium access control layer

.

Advantages

- Its secure communication framework provides a technique to verify data in line and drop false packets from malicious nodes, thus maintaining the health of the wireless network.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

- It dynamically updates keys without exchanging messages for key renewals and embeds integrity into packets as opposed to enlarging the packet by appending message authentication codes (MACs).
- The key to the encryption scheme (RC4) dynamically changes as a function of the residual virtual energy of the node, thus requiring no need for rekeying.
- The protocol is able to continue its operations under dire communication cases as it may be operating in a high-error-prone deployment area like under water.

System architecture

The framework is comprised of three modules: Node Energy-Based Encoding, Crypto, and Forwarding shown in fig1. The virtual energy-based keying process involves the creation of dynamic keys. Contrary to other dynamic keying schemes, it does not exchange extra messages to establish keys. A sensor node computes keys based on its residual virtual energy of the sensor. The key is then fed into the crypto module.
The crypto module in ENEBE and FFDI employs a simple encoding process, which is essentially the process of permutation of the bits in the packet according to the dynamically created permutation code generated via RC4. The encoding is a simple encryption mechanism adopted for ENEBE and FFDI However, ENEBE and FFDI s flexible architecture allows for adoption of stronger encryption mechanisms in lieu of encoding. Last, the forwarding module handles the process of sending or receiving of encoded packets along the path to the sink.

Keying module ensures that each detected packet is associated with a new unique key generated based on the constantly changing value of the energy. The dynamic key is generated by using algoritham1, it is passed to the RC4 encryption module (crypto module), where the desired security services are implemented. The process of key generation is initiated when data is sensed, thus no explicit mechanism is needed to refresh or update keys. Because of the dynamic nature of the keys it makes difficult for attackers to prevent enough packets to break the encoding algorithm. Each node computes and updates the constantly changing value of its energy after performing some actions.

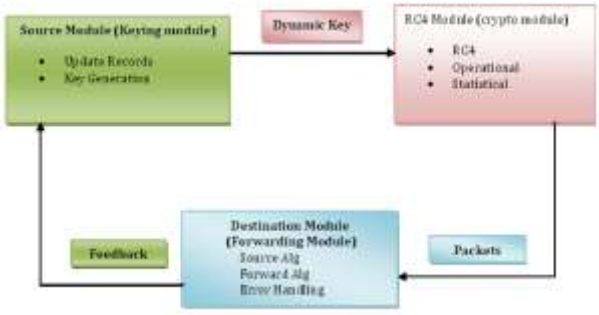

Figure1. Architecture Model for ENEBE and FFDI

➢ Dynamic key generation algorithm

Algorithm1: Compute Dynamic Key
ComputeDynamicKey(masterkey,packetsize)
begin
j← temp;
if j → 1 then
K ←dynamickey(masterkey,packetsize)
else
K ← dymamickey(kj-1, masterkey)
end if
return K
end

➢ Crypto Module

The RC4 (Crypto) module uses a simple encoding process, which is essentially the process of permutation of the bits in the packet according to the dynamically created permutation code generated via RC4. The encoding is a simple encryption mechanism adopted for ENEBE and FFDI. However, ENEBE and FFDI's flexible architecture allows for stronger encryption mechanisms in lieu of encoding

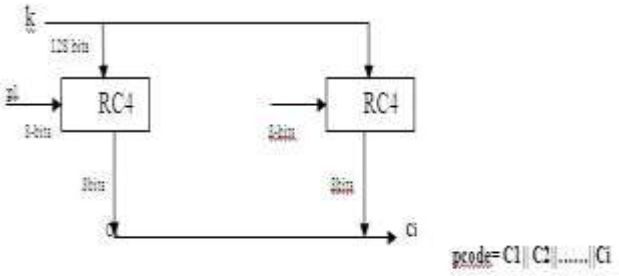

Figure2: RC4 encryption mechanism in ENEBE and FFDI

Each action on a node is associated with a certain predetermined cost. Since a node will be either forwarding some other nodes data or injecting its own data into the network, the set of actions and their

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

associated energies for ENEBE and FFDI includes packet reception, packet transmission, packet encoding, packet decoding energies, and the energy required to keep a node alive in the idle state.

- **Forwarding Module**
  The forwarding module handles the process of sending or receiving of encoded packets along the path to the sink.

Source node
The source node uses the local energy value and an initialization vector (IV) to construct the next key.

The key is used as input into the RC4 algorithm inside the crypto module to create a permutation code for encoding the *{ID,type,data}*message.
The encoded message and the clear text ID of the originating node are transmitted to the forwarding node or Sink using the following format: *{ID{ID,type,data}}Pc.*

Forwarding Node
Once the forwarding node receives the packet it will first check its watch-list.

If the node is not being watched by the current node, the packet is forwarded without modification or authentication and its local perceived energy value is not updated.
If the node is being watched by the current node, the forwarding node checks the associated current energy record stored for the sending node and extracts the energy value to derive the key.
It then authenticates the message.
If the packet is authentic, an updated energy value is stored in the record associated with the sending node.
If the packet is not authentic it is discarded. Again, the energy value associated with the current sending node is only updated if this node has performed encoding on the packet.

Addressing communication error handling
Communication errors may cause some of the packets to be lost or dropped and malicious packets inserted by attackers. To solve potential loss of packets due to possible communication errors in the network, all the nodes are configured to store an additional energy value, which we refer to as the bridge energy. This bridge energy value allow resynchronization of the network, determines that packets were lost.

Operational modes

OM-I (ENEBE)
In the OM-I operation, all nodes watch their neighbors; whenever a packet is received from a neighbor sensor node, it is decoded and its authenticity and integrity are verified. Only legitimate packets are forwarded toward the sink. During this period, route initialization information may be used by each node to decide which node to watch and a record r is stored for each of its one-hop neighbors in its watch-list. To obtain a neighbor's initial energy value, a network-wise master key can be used to transmit this value. Alternatively, sensors can be preloaded with the initial energy value.

If the forwarding node is not able to extract the key successfully, it will decrement the predefined energy value from the current perceived energy and tries another key before classifying the packet as malicious This process is repeated several times; however, the total number of trials that are needed to classify a packet as malicious is actually governed by the value of Key Search Threshold. OM-I reduces the transmission overhead as it will be able to catch malicious packets in the next hop. If the packet is authentic, and this hop is not the final hop, the packet is reencoded by the forwarding node with its own key derived from its current virtual bridge energy level. If the packet is illegitimate, the packet is discarded. This process continues until the packet reaches the sink. Reencoding at every hop refreshes the strength of the encoding. The general packet structure is {ID{ID; type; data}}.

OM-II (Filtering of False Data Injection -FFDI).
In the OM-II operation, nodes in the network are configured to only watch some of the nodes in the network.
Each node randomly picks r nodes to monitor and stores the corresponding state before deployment. As a packet leaves the source node it passes through node(s) that watch it probabilistically. Thus, OM-II is a statistical filtering approach like SEF and DEF.

If the current node is not watching the node that generated the packet, the packet is forwarded. If the node that generated the packet is being watched by the current node, the packet is decoded and the plaintext ID is compared with the decoded ID. Similar to function of OM-I, and continues until the packet reaches the sink.

This operational mode has more transmission overhead because packets from a malicious node may or may not be caught by a watcher node and they may reach the sink. However, compare to the OM-I mode, it reduces the processing overhead because less re-encoding is

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

performed and decoding is not performed at every hop. The trade-off is that an illegitimate packet may traverse several hops before being dropped.

In OM-I and OM-II, in order for an attacker to be able to successfully inject a false packet, an attacker must forge the packet encoding (which is a result of dynamically created permutation code via RC4). Given that the complexity of the packet is 2l, where l is the sum of the ID, TYPE, and DATA fields in the packet, the probability of an attacker correctly forging the packet.

Accordingly, the probability of the hacker incorrectly forging the packet, and therefore, the packet being dropped (pdrop_I)

Since OM-I authenticates at every hop, forged packets will always be dropped at the first hop with a probability of Pdrop_I . OM-II statistically drops packets along the route.

Mathematical Concepts

Single cost (E_{so}) to stay-alive, sense the event, encode the packet and transmit the packet (E_{sa} ,E_{sens} , E_{sens} ,E_{tx}) at the source sensor,

$$E_{so} = E_{sens} + E_{encr} + E_{tx} + E_{sa}$$

Forwarding cost (E_{FWD}) to marshal the packet through the network depending on the number of hops,

$$E_{FWD} = E_{rx} + E_{decr} + E_{encr} + E_{tx} + E_{sa}$$

The probability of an attacker correctly forging the packet is,

$$P_{forge} = \frac{1}{2^{packet\ size}}$$

The packet being dropped ($P_{drop\text{-}I}$) is,

$$P_{drop-i} = 1 - P_{forge}$$

Notations:
Esa: Stay Alive.
Esens: Sense the event.
Eencr: Encoding the packet.
Etx: Transmit packet.
Efwd: Forwarding energy.
Erx: Receiving packet.
Edecr: Decrypting the packet.

Performance analysis

We are plotting a graph across the hops which involved in communication and energy. A graph is developed in two dimensional, hop represents x –axis and an energy in y-axis.

Communication across the sensor node is major dominant factor, because it consumes more cost. As seen in the resulting graph our proposed method ENEBE and FFDI achieves the less energy consumption as compare to the existing method STEF. The same result is shown in figure.

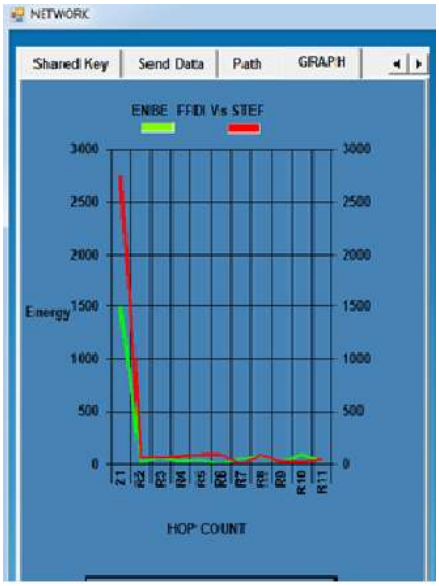

Figure3: Performance Analysis graph

Conclusion and future work

Communication is very costly for any network. Independent of the goal of saving energy, it may be very important to minimize the exchange of messages (e.g., military scenarios). To address these concerns, we presented a secure communication framework called Node Energy- Based Encryption and Keying. In comparison with other key management schemes, Efficient Node Energy Based Encoding(ENEBE) and Filtering of False data Injection(FFDI) has the following benefits: 1) it does not exchange control messages for key renewals and is therefore able to save more energy and is less chatty, 2) it uses one key per message so successive packets of the stream use different keys—making NEBE and FFDI more resilient to certain attacks (e.g., replay attacks, brute-force attacks, and masquerade attacks), and 3) it unbundled key generation from security services, providing a flexible modular architecture that allows for an easy adoption of different key-based encryption or hashing schemes. Renewals and is therefore able to save more energy and is less.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

References

1. 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.
2. C. Kraub, M. Schneider, K. Bayarou, and C. Eckert, "STEF: ASecure Ticket-Based En-Route Filtering Scheme for Wireless Sensor Networks," Proc. Second Int'l Conf. Availability, Reliability and Security (ARES '07), pp. 310-317, Apr. 2007.
3. G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors," Comm. ACM, vol. 43, no. 5, pp. 51-58, 2000 Computerworld.
4. H. Hou, C. Corbett, Y. Li, and R. Beyah, "Dynamic Energy-Based and Filtering in Sensor Networks", Proc. IEEE Military Comm. Conf. (MILCOM '07), Oct. 2007.
5. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filteringof Injected False Data in Sensor Networks," IEEE J. Selected Areas in Comm., vol. 23, no. 4, pp. 839-850, Apr. 2005.
6. Huy Hoang Ngo, Xianping Wu, Phu Dung Le, mpbell Wilson, and Balasubramaniam Srinivasan ,"Dynamic Key Cryptography and Applications," Monash University,900 Dandenong Road, Caul¯eld East,Victoria, 3145, Australia Feb. 9, 2009.
7. Raheem A. Beyah, Yingshu Li, John A "Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks".