*Grenze International Journal of Engineering and Technology, Jan 2017*

# Hop by Hop Virtual Energy based Authentication Scheme for Wireless Sensor Network

Er.Kusum[1], Er.Sanjeev Kumar[2] and Ankush Gupta[3]
[1]Assistant Professor/CSE ,MMU, Mullana,Ambala,INDIA
Email: { kusumchaudhary1@gmail.com }
[2-3] Assistant Professor/YIET/EED, YAMUNANAGAR, INDIA
Email: {sanjeevchoudhary38@gmail.com}

***Abstract*—A Wireless Sensor Networks is a large network of resource-constrained sensor nodes with multiple preset functions, such as sensing and processing, to fulfil different application objectives. Usually, sensor nodes are deployed in a designated area by an authority such as the government or a military unit and then automatically form a network through wireless communications. Designing cost-efficient, secure Wireless Sensor Networks is a challenging problem because sensors are resource-limited wireless devices. Since the communication cost is the most dominant factor in a sensor's energy consumption, so the proposed work introduce an energy-efficient Secure Virtual Energy-Based Hop by Hop dynamic key Encryption scheme for WSNs which reduces communication overheads required to exchange the messages to update the dynamic key in the network. In the proposed work a key used in the encryption or decryption function changes dynamically by using the concept of virtual energy. The virtual energy (VE) is a numeric value that is assign to each node before the deployment of network. This VE changes dynamically whenever a function is performed by the node in the network. Thus, a one-time key is used to encode one packet only and different keys are used for other packets. The receiving node known as watch node (WN), will calculate the key used in decryption process as a predicted value as the same value used by the sending node in the encryption process. So with the help of this predicted value, the receiving node is able to verify the integrity and authenticity of the message. Thus there is no need for the communication of extra control messages to update the dynamic key. The problem with the existing schemes to generate a dynamic key with the help of a virtual energy is that every time the predicted value is generated, the same amount of value is decremented in each function but in proposed scheme this value dynamically changes as a function over time. So it is impossible for intruder to know the key value of any node. Simulation result proves that the proposed scheme is more secure than other scheme in the same area.**

***Index Terms*— Security, WSN Security, Dynamic key encryption, Virtual energy based keying.**

## I. Introduction

A WSN is a large network of resource-constrained sensor nodes with multiple preset functions, such as sensing and processing, to fulfil different application objectives. Usually, sensor nodes are deployed in a

*Grenze ID: 01.GIJET.3.1.30*

designated area by an authority such as the government or a military unit and then automatically form a network through wireless communications. Sensor nodes are static most of the time, whereas mobile nodes can be deployed according to application requirements. One or several base stations (BSs) are deployed together with the network.  Sensor nodes keep monitoring the network area after being deployed. After an event of interest occurs, one of the surrounding sensor nodes can detect it, generate a report, and transmit the report to a BS through multi hop wireless links. Collaboration can be carried out if multiple surrounding nodes detect the same event. In this case, one of them generates a final report after collaborating with the other nodes. The BS can process the report and then forward it through either high-quality wireless or wired links to the external world for further processing.

## II. SYSTEM MODEL

The system model of proposed work is divided into three different modules. Virtual energy based dynamic key module that create the dynamic key that is then send into the crypto module.

a. Crypto module that perform the encryption and decryption function to generate the authenticated code to provide the confidentiality of the packets.
b. Forwarding module is the third module that performed some function. The Modular structure of secure virtual energy based dynamic key encryption is shown in Fig.1

### *A. Virtual Energy Based Dynamic Key Module*

The virtual energy based dynamic keying module is one of the primary contributions of this chapter. It is essentially the method used for handling the keying process. It produces a dynamic key that is then fed into the crypto module. After deployment, sensor nodes traverse several functional states. The states mainly include node-stay-alive, packet reception, transmission, encoding and decoding. In this case, the following is the virtual cost associated with the source node:

$$VC = N*(eTX + eENC) + (t*eA) + (N*(eRX + eDEC) + eA*t) \qquad (1)$$

In the case where a node receives data from another node, the virtual perceived energy value can be updated by decrementing the cost associated with the actions performed by the sending node using the following cost equation. Thus, assuming that the receiving node has the initial virtual energy value of the sending node and that the packet is successfully received and decoded associated with a given source sensor, k, and the virtual cost of the perceived energy is computed as follows:

$$VPE = N*(eTX + eENC + eRX + eDEC) + (2*eA*t) \qquad (2)$$

### *B. Crypto Module*

In this section introduce a simple encoding operation similar to that used in previous work. The encoding operation is essentially the process of permutation of the bits in the packet according to the dynamically created permutation code via the encryption mechanism. The purpose of the crypto module is to provide simple confidentiality of the packet.

***Encryption Algorithm:*** In this algorithm discuss a very simple encoding process that can be used to ensure the authenticity and confidentiality of sensed data without incurring transmission overhead. In this scheme uses a keyed encryption approach, each node sends its ID, type and data to its next hop.

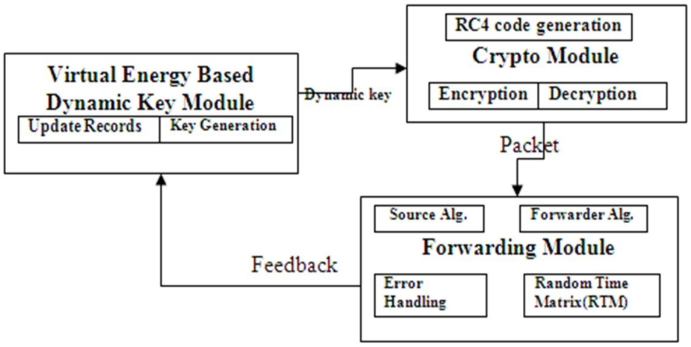

Figure 1. Modular structure of secure virtual energy based dynamic key encryption

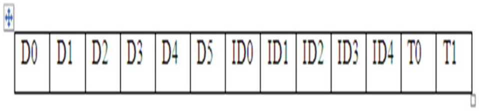

Figure 2. Format of different Keys

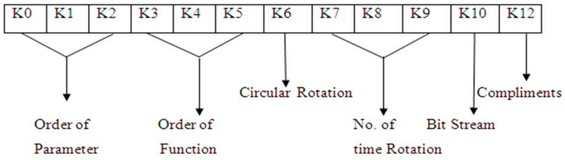

Figure 3. Different parameter used in key

The format of the packet to be transmitted shown in fig 2, becomes:
Bit Stream Packet = {id, type, data} k
The computed code is used to encode the <id\type\data> message.
The format of the packet to be transmitted shown in fig 3, becomes:

Packet = {id, type, data} k

The encryption algorithm can be mapped to a set of actions to be taken on the data stream combination. The action can include:

1. Order of Parameters
   ID, T, D – 000
   ID, D, T – 001
   T, ID, D – 010
   T, D, ID – 011
   D, ID, T – 100
   D, T, ID – 101
2. Order of Function
   CR, BS, C – 000
   CR, C, BS – 001
   BS, CR, C – 010
   BS, C, CR – 011
   C, CR, BS – 100
   C, BS, CR – 101
3. Circular Rotation
   LEFT – 0
   RIGHT – 1
4. No. of time Rotation
   000 - 111
   Left to Right – 0
   Right to Left– 1
5. Compliments
   Enable – 1
   Disable – 0

### *C. Forwarding Module*

The final module in the system model is the forwarding module. The forwarding module is responsible for the sending of packets or received packets from other sensors (forwarding nodes) along the path to the BS. The operations of the forwarding module are explained in this subsection.

*Source Node Algorithm:* When an event is detected or sensed by a node the next step is for the packet to be secured. The sensed node uses the virtual energy value and an IV (or previous key value if not the first transmission) to construct the next key.

*Forwarder Node Algorithm: O*nce the forwarding node receives the packet it will first check its watch-list to determine if the packet came from a node it is watching. If the node is not being watched by the current node, the packet is forwarded without modification or authentication.

*Error Handling: I*n this to authenticate a packet, a node must keep track of the virtual energy of the sending node to derive the key needed for decoding.

*Random Time Matrix (RTM) algorithm:* In the Forwarding Module the Random Time Matrix algorithm described the two functions: Fix Time Generation function and Random Time Generation function. The use of random time generation function is to generate the random key for sending and receiving of the packets. The representation of this function is described in the matrix form that is shown in fig 4:

Where $T_{ij}\rightarrow$ is the event detected by sensor node i at time j.

$Td_{ij}$ → is the time difference when the event is detected by sensor node i at time j and the time when the previous event is detected by same sensor node i at j-1 time.

### *D. Relationship between key updating of different sensors*

In this proposed work the different dynamic key is used by the every node. The watching concept is illustrated with an example in Fig 5. In the below figure, there is one source sensor node, A, and other nodes B, C, D and E are located along the path to the sink. Every node watches its downstream node, i.e., B watches A (B $\bar{w}$ A), C watches B (C $\bar{w}$ B), D watches C (D $\bar{w}$ C) and E watches D (E $\bar{w}$ D).

## III. System Implementation

In this the algorithm used for the proposed work is defined, which gives the information to find optimal path between source and destination.

### *A. Generation of Dynamic key*

In this the virtual energy-based keying process involves the creation of dynamic keys. It does not exchange extra messages to establish keys. A sensor node computes dynamic keys based on its residual virtual energy of the sensor. After deployment of sensor nodes traverse several functional states. As each of these actions occurs, the virtual energy in a sensor node is depleted.

### *B. Forwarding node with communication error handling*

The next section explains the process of forwarding module, this section handles the process of sending or receiving of encoded packets along the path to the base station i.e., sink. Once the forwarding node receives the packet it will first check its watch-list to determine if the packet came from anode it is watching. If the node is not being watched by the current node, the packet is forwarded without modification or authentication. Although this node performed actions on the packet, its local virtual perceived energy value is not updated. This is done to maintain synchronization with nodes watching it further up the route.

$$\begin{matrix}
T_{11} & T_{12} & T_{13} & \cdots & T_{1(i-1)} & T_{1i} & T_{1(i+!)} & \cdots & T_{n} \\
T_{21} & T_{22} & T_{23} & \cdots & T_{2(i-1)} & T_{2i} & T_{2(i+1)} & \cdots & T_{n} \\
. & . & . & \cdots & . & . & . & \cdots & . \\
. & . & . & \cdots & . & . & . & \cdots & . \\
T_{(j-1)1} & T_{(j-1)2} & T_{(j-1)3} & \cdots & T_{(j-1)-1} & T_{(j-1)i} & T_{(j-1)i+1} & \cdots & . \\
T_{j1} & T_{j2} & T_{j3} & \cdots & T_{j(i-1)} & T_{ji} & T_{j(i+1)}[\,|\,|] & \cdots & . \\
. & . & . & \cdots & . & . & . & \cdots & . \\
. & . & . & \cdots & . & . & . & \cdots & .
\end{matrix}$$

Figure 4. The representation of the function in matrix form

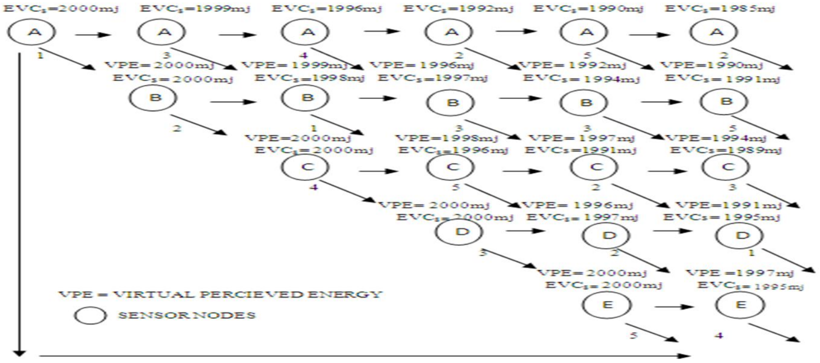

Figure 5. Relationship between key updating of different sensors

### *C. Generation of Random Time Matrix*

In random time matrix generation algorithm it makes the matrix in which it takes the key value randomly. Let we have number of nodes then the nodes get the value from that matrix which has already predefined random key value. By using this matrix once the node forwarded the packet, then every time each node has their perceived value will come different. If an intruder get the one key then it is impossible to get the next and previous key value of any node.

Algorithm: Random Time Matrix (RTM) Generation algorithm

```
Step1: Create RTM (IDclr,T,no of nodes)
Step2: begin
Step3: row ← j=0, cols ← 0 to i
Step4: if row < no of nodes   then
Step5: j++
Step6: elseif cols< i then
Step7: i ++
Step8: endif
Step9:  t ← r.next (j)
Step10:  randomTime ← t
Step11:  endif
Step12:  create getTime(id, m)
Step13:  index ← -1, i=0
Step14:  if i< no of nodes   then
Step15:if  nodes.get(i)=id   then
Step16:  index=i
Step17:  i++
Step18:  endif
Step19:  endif
Step20:t ← m%5
Step21:   return RTM (index,t)
Step22:   end
```

## IV. Result and Discussion

### *A. Design of network with some parameter*

The table1 shows the different parameter with values for design of network. If we consider 10 number of nodes, then the transmission and receiving energy is 50*0.0000000001nl/bit and for decoding, encoding energy is Pktsize*0.000000001nj. After the deployment of network the initial virtual energy (eINI) is 0.02nj/node. In the proposed work a key used in the encryption or decryption function changes dynamically by using the concept of virtual energy. When an action performed by each node then the virtual energy is decreases dynamically. After performing some action, each node will give different virtual energy called virtual perceived energy (VPE) and self virtual cost energy (EVCs). The virtual energy (VE) is a numeric value that is assign to each node before the deployment of network

### *B. The result in form of graphical representation*

The graphically result show the difference between both model. In the previous model the value of virtual perceived energy is same for every node in one round but in our proposed model the value of virtual perceived energy is different for each node in one round which is shown in fig 6. In the below result the x-axis shown number of nodes and the y-axis shown the virtual energy. The red line show the result of virtual perceived energy in previous model and blue line show the result of virtual perceived energy in the proposed model that is different for each node in every round.

### *C. Abbreviations and Acronyms*

Wireless Sensor Networks (WSNs), Virtual Energy (VE) , Watch Node (WN), Base Stations (BSs), Virtual Energy-Based Encryption and Keying (VEBEK), Virtual Energy-Efficient Encryption and Keying (VEEEK), Packet Reception (eRX), Packet Transmission (eTX), Packet Encoding(eENC), Packet Decoding Energies(eDEC), Virtual Perceived Energy (VPE), Random Time Matrix (RTM)

TABLE I. ENERGY RELATED PARAMETERS

| Parameter | Value | Parameter | Value |
|---|---|---|---|
| *eTX* | 50*0.000000001nj/bit | eDEC | Pktsize*0.000000001nj |
| *eRX* | 50*0.000000001nj/bit | eENC | Pktsize*0.000000001nj |
| *eA* | 0.000000001nj | eINI | 0.02J/node |
| Pktsize | N bit | eaINI | 0.02J/node |

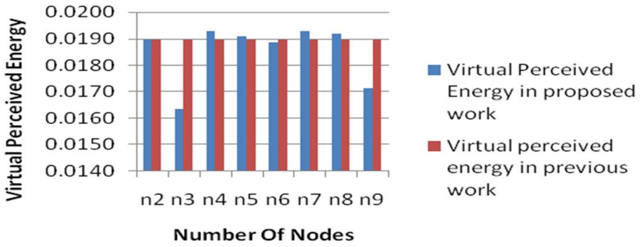

Figure 6. Comparision between previoud model and proposed model

## V. CONCLUSION

The proposed work introduce an energy-efficient Secure Virtual Energy-Based dynamic key Encryption scheme for WSNs which reduces communication overheads required to exchange the messages to update the dynamic key in the network. In the proposed work a key is used in the encryption or decryption function changes dynamically by using the concept of virtual energy. This VE changes dynamically whenever a function is performed by the node in the network. Thus, a one-time key is used to encode one packet only and different keys are used for other packets. The receiving node known as watch node (WN), will calculate the key used in decryption process as a predicted value as the same value used by the sending node in the encryption process. So with the help of this predicted value, the receiving node is able to verify the integrity and authenticity of the message. Thus there is no need for the communication of extra control messages to update the dynamic key. Simulation result proves that the proposed scheme is more secure than other scheme in the same area.

## REFERENCES

[1] Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." In Advanced Communication Technology, 2006.ICACT 2006.The 8th International Conference, vol. 2, pp. 6-pp. IEEE, 2006.

[2] Walters, John Paul, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. "Wireless sensor network security: A survey." Security in distributed, grid, mobile, and pervasive computing 1 (2007): 367.

[3] Naeem, Tahir, and Kok-Keong Loo. "Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks." 3; 1(2009).

[4] Du, Wenliang, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K. Varshney. "A key management scheme for wireless sensor networks using deployment knowledge." In INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 1. IEEE, 2004.

[5] Du, Wenliang, Jing Deng, Yunghsiang S. Han, and Pramod K. Varshney. "A pairwise key pre-distribution scheme for wireless sensor networks."InProceedings of the 10th ACM conference on Computer and communications security, pp. 42-51.ACM, 2003.

[6] Chan, Haowen, Adrian Perrig, and Dawn Song. "Random key predistribution schemes for sensor networks."In Security and Privacy, 2003.Proceedings. 2003 Symposium on, pp. 197-213. IEEE, 2003.

[7] [7] Krishnaja, K. Naga, and MHM Krishna Prasad. "SVE: Security using Virtual Energy for Wireless Sensor Networks"

[8] Chythanya, K. Ravi, S. P. Anandaraj, and S. Padmaja. "Virtual Energy-Efficient Encryption and Keying (VEEEK) for Wireless Sensor Networks." International Journal 3 (2011).