# Data Encryption in the Hostile Environment for Wireless Sensor Network Using Virtual Energy and Trigger Time Response Protocol

**Krishan Kant Lavania[1], Saumitra Mani Tiwari[2] and Sahil Batra[3]**

**[1] Head, Department of Information Technology, Arya Institute of Engineering & Technology
Jaipur, India**

**[2] Student, Department of Information Technology, Arya Institute of Engineering & Technology
Jaipur, India**

**[3] Student, Department of Information Technology, Arya Institute of Engineering & Technology
Jaipur, India**

## Abstract

The future of communication is the intelligent sensors capable enough to manage the decision making process by making communication among themselves. Although to do that they need a secure communication to take place which is continuous and for that we need energy sources which is continuous and always flowing in. This is a major problem as making any communication safe today is a complex process as the intruders today are very much advanced and nothing less than implementing a proper Encryption algorithm to secure the data, it is not safe and to that we need to keep energy flowing to keep encryption engines running. The Whole concept is the need for Future Technology and Virtual Energy Based Encryption (VEBEK) is the answer for that. VEBEK is a secure communication framework in which permutated key generated by RC4 encryption mechanism is used for encryption. The Key to RC4encryption changes dynamically in accordance to the residual energy packets of the Sensor. Thus every data packet has a different dynamically generated key coming in succession. And keying messages send to different ends are also not needed for checking the authenticity as the nodes present in between the path of network of sensors does that, making the communication authenticated and integrated.

## 1. Introduction

Wireless Sensor Technology has become the technology that can be applied in more and more fields of applications. Apart from the typical Areas like Environmental, Military and Commercial Enterprise. Where we can see them in surveillance, Oceanographic data collection, pollution monitoring, navigation assistance etc. Further Improvements in the sensors can evolve the sensors to be a part of our daily life, doing more work than only capturing a data for alerting.

Here as the field of application for the sensor will increase, there will be increase in the need of accuracy and authenticity of the data they would provide, so that the monitoring of the critical section can be used on an immediate basis to carry out the actions (e.g. deployment and control of man-less planes like drones). And also the security of the signals exchanged has to be maintained under a resilient protocol to prevent malicious code producing false data, which can result in serious consequences of heavy data and money loss.

The Security of sensor network is a dire task as these wireless devices are small in size and are deployed in large numbers, usually in a hostile environment and have the limit in which they can carry the resource (e.g. power source to keep sensors running, computational capacity and memory to store it). For Example a typical sensor operates at a frequency of 2.4 GHz, has a data rate of 250 Kbps, 128 KB of program memory 512 KB of memory of measurement transmit power of 1mW, and communication range of 30m to 100m. Thus the resource usage on field has to be most efficient.

This paper focuses on the keying mechanism based on two fundamental schemes for WSN which are Static and Dynamic. In static the key Management functions (key generation and distribution) are carried prior to or shortly after network deployment, keeping the number of keys to be loaded fixed. While in dynamic keying key is changed at the time of communication. Dynamic keys are more attack resilient as the whole message is difficult to get decoded due to each packet having different key unlike in static, however their power consumption is also very high, as more amount of message are to be passed in case of exchanging the keys every time. So for that we keep a note to minimize the overhead associated with the refreshing key to maintain the efficiency of the sensor. As the communication cost is among the most dominant factor to check in sensor technology, the keying of message has to be checked to ensure the energy utilization is optimum. Apart from that in applications like Military Surveillance, spying etc. we prefer the number of messages to be passed to be minimum in count making them even harder to get detected while being present in enemy lines.

This paper throws light on VEBEK (Virtual Energy Based Encryption and Keying). Its framework provides a technique to verify data in line and get rid of packets containing malicious codes thus dynamically updating keys without any key exchange of messages. We can see that this type of encryption provides us with all the necessary features needed from an efficient way for sensor networks.

## 2. Background of Keying

Efficient Key management schemes is needed to be done to make keys available to communicating nodes (Source and Sink) for maintaining aspect of confidentiality. The Providence of Keys to the sensors has to be done before deployment of network or at the time of triggering when the keys can be redistributed. The key given before the network deployment is called the static key while the later is known as dynamic key. The VEBEK only makes use of dynamic keying as by this it saves the energy that would have been wasted in sending the messages to the sink and source to keep a list of keys used for Encryption.

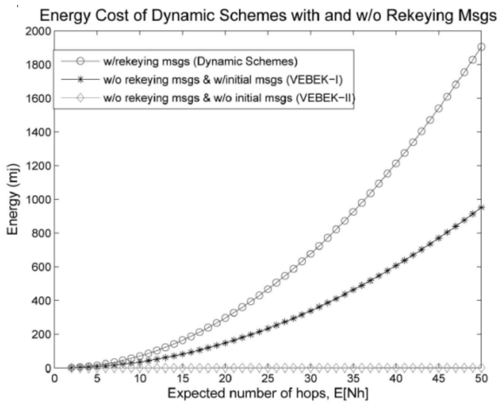


Fig1: Energy consumption for Keying in Dynamic Energy based schemes (VEBEK-I and VEBEK-II)

The Keying in VEBEK is done in two operational modes (VEBEK-I and VEBEK-II), The detail about both of them would be discussed in later part of the paper, however we keep a note that in VEBEK-I there is no rekeying of messages in a dynamic system though there is some initial information exchange in the neighborhood, while In VEBEK-II there is no exchange of message before, though we have a dynamic system having no keying of messages.

The Figure given on right hand side shows the analysis of the result from the expressions given above, and we can see that for both VEBEK modes the cost of Energy components would be fixed, although for VEBEK-I we also include cost of messages sent before the transmission showing its energy lower than VEBEK-II. Here we can see that large amount of energy is consumed in rekeying of messages, and how VEBEK provides us with an efficient encryption but on a lower energy consumption benefit. Also here the energy is mainly consumed in generating random keys for the packets in dynamic environment making the VEBEK resilient to attacks like Brute Force Attacks, Replay Attacks and Masquerade attacks.

## 3. Structure of VEBEK Frameworks

The VEBEK framework comprises of three modules: Virtual Energy Based Keying, Crypto and Forwarding. In this the Virtual Energy Based Keying process involves the work to create Dynamic Keys without sending extra message to establish keys. The Key here is calculated based on the Virtual Energy of the sensor; the key is then fed to crypto module to do the encoding part.

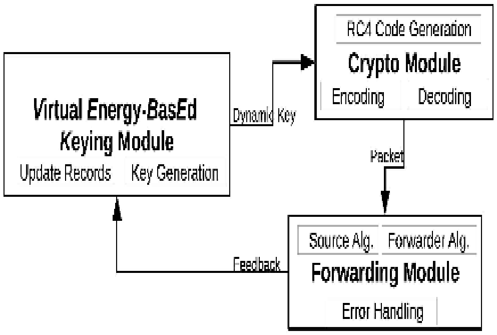
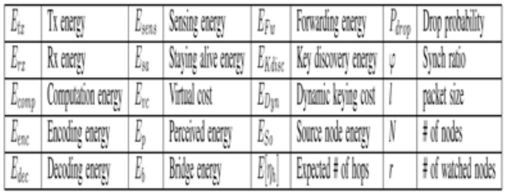


Fig 2: Modules of Vebek Framework

The Crypto part of the Framework does the simple encoding process, which is actually a process of permutation of bits present in a packet, in accordance to the dynamically generated code with help of RC4. The encoding here is told as simple, however there can be stronger encryption mechanism used in the flexible VEBEK framework for better security. Here the sending and receiving of forward module is handled by the forwarding module.

## 3.1 Virtual Energy Based Keying Module

The Virtual Energy Based Keying Module is the method used for handling the keying process. It produces a dynamic key to be fed in the crypto module, which are based on the value of virtual energy present in a particular sensor node at that moment. The Ratio of difference between the adjacent batteries can vary in this process and can result in dropping of some packet; VEBEK keeps a check on this problem too. Now the Sensor nodes after getting active traverse various functional states, like packet reception, transmission, encoding, decoding and node-stay-alive. As each of these states occurs the virtual energy of the sensor gets timid. The Current value of the virtual energy given by EVC is used for generating the key by generation function F. During the initial phase all nodes have same energy level Eini, thus the key K1 is the function of initial virtual energy value and the initial vector IV which are pre distributed to the sensors. Subsequently key Kj is the function of the current value Evc and the previous key Kj-1. Thus in this way VEBEK ensures that each packet has a dynamic key generated with the help of its current value of Virtual Energy and the Key present on its previous node and passing it as the key to Crypto Module doing encoding safe from different types of attacks.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $E_{tx}$ | Tx energy | $E_{sens}$ | Sensing energy | $E_{Fw}$ | Forwarding energy | $P_{drop}$ | Drop probability |
| $E_{rx}$ | Rx energy | $E_{sa}$ | Staying alive energy | $E_{Kdisc}$ | Key discovery energy | $\varphi$ | Synch ratio |
| $E_{comp}$ | Computation energy | $E_{vc}$ | Virtual cost | $E_{Dyn}$ | Dynamic keying cost | $l$ | packet size |
| $E_{enc}$ | Encoding energy | $E_p$ | Perceived energy | $E_{S_0}$ | Source node energy | $N$ | # of nodes |
| $E_{dec}$ | Decoding energy | $E_b$ | Bridge energy | $E[\eta_h]$ | Expected # of hops | $r$ | # of watched nodes |

Table 1: Notations Used in VEBEK

Each Sensor Node Computes its key with the help of the value of the virtual energy present at any instant , and there are also number of values of energy consumed in different processes like Energy for Packet reception (Erx) , Packet Transmission(Etx), Encoding(Enc), (Edec) for decoding so all types of energies are mentioned in the table given above.

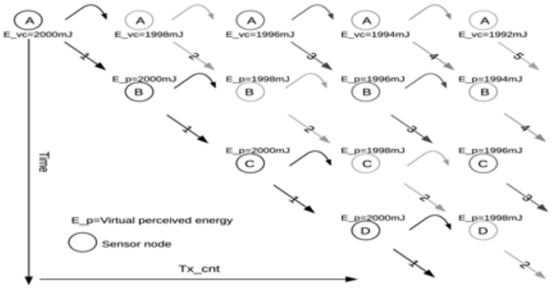


Fig3. The Process of Watching and Forwarding

To be precise the instantaneous value of the virtual energy, EV is computed by decrementing the total of the predefined value Evc, from the previous virtual energy value. However if the sensor node is just a forwarder ( only a intermediate receiver between two nodes) the successful decoding and authentication the receiving node keep track of the energy of the sending node to keep derive the key for decoding. In VEBEK the process of tracking the virtual energy of sending node is called watching, and the energy value associated with it is called Virtual Perceived Energy (Ep).

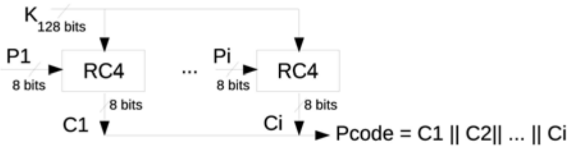


Fig 4: RC4 encryption mechanism in VEBEK

## 3.2 Crypto Module

Due to the constraint to make use of less amount of energy the encoding algorithm in Wireless Sensor Networks has to be kept bvetry simple but also effective. Here in VEBEK we generally make use of RC4 encryption mechanism. It works on the base of creating a permutation of the bits in the packet with the dynamic key provided by the previous node by energy based keying module. The process is kept simple as to save energy of the battery being used although if needed complex algorithm can also be used in it to provide enhanced security as VEBEK provides us with the flexibility to do that. The packets in the VEBEK consists of ID (i bits),Type (t bits) and data bit fields. Each Node sends these to next hop, however the sensors ID type and the sensed data is send in pseudo random type in accordance to the result of RC4.More Specifically the RC4 algorithm takes the data byte by byte as input and produces result as permutated code. The concatenation of every 8 bits of output becomes a permutation code. Due to the constraint to make use of less amount of energy the encoding algorithm in Wireless Sensor Networks has to be kept bvetry simple but also effective. Here in VEBEK we generally make use of RC4 encryption mechanism. It works on the base of creating a permutation of the bits in the packet with the dynamic key provided by the previous node by energy based keying module. The process is kept simple as to save energy of the battery being used although if needed complex algorithm can also be used in it to provide enhanced security as VEBEK provides us with the flexibility to do that. The packets in the VEBEK consists of ID (i bits),Type (t bits) and data bit fields. Each Node sends these to next hop, however the sensors ID type and the sensed data is send in pseudo random type in accordance to the result of RC4.More Specifically the RC4 algorithm takes the data byte by byte as input and produces result as permutated code. The concatenation of every 8 bits of output becomes a permutation code.

## 4. **Working Modes of VEBEK**

Authentication, non repudiation and Integrity are some among the Security Services provided by the VEBEK protocol. The Base of these services is the Watching mechanism discussed earlier. And the data retrieved by it to be stored in the memory to be further used in services. But there is cost involved in storing data, communication and computation like purposes, and these can vary according to the requirement of the purpose involved, for example the cost of surveillance for military has to be more than determining the temperature of a national park that comes in a civilian work. The VEBEK framework keeps note of the requirement and provides flexibility according to needs thus supporting two modes of working VEBEK-I and VEBEK-II, The detail About Both Are given below.

### 4.1 VEBEK-I

IN VEBEK-I all operational nodes watch their neighbors, whenever a packet is received from their neighbor they decode it and verifies its authenticity, Only tested packets are forwarded towards the sink cutting short all the packets infected by malicious codes by any means. In this mode we assume existence of a window of time at initial deployment that an adversary is not able to compromise the network, as it will take time for an attacker to capture the keys that would be needed to decode the packet. During this time route initialization information is used by other nodes to make decision which node to watch and after every watch a record a is stored for the watch list of each of its neighbors. Now to obtain the initial value of any of the neighbor a master key can be used to transmit this value during the time of sharing it as it is always the same for every node. As the time passes the function F determines the key based upon the different types of Energies involved in the process of depleting the value virtual energy.

When the Packet reaches next hop node the key of the seeding node is extracted by forwarding node from its records and the value of virtual energy of the packet is used to decode it to obtain the value. After decoding the plain text ID is compared with the decoyed ID. This process is done several times decreasing the value of virtual energy to find out the decoded ID, and if there is a fault found the malicious code is detected and so the packet is discarded. The number of check perform to determine the malicious code vary in accordance. But is governed by the value of virtual key threshold, and if the Packet is Authentic it is forwarded towards the sink.

### 4.2 VEBEK-II

In the VEBEK-II nodes are configured to watch only some nodes in the network. Each Packet Picks up a random node to monitor and stores its state before leaving. As the packet moves from different nodes where it is watched on the basis of randomization .VEBEK-II follows statistical filtering procedure in which the current node is not watching the node which has generated then the packet is forwarded. And IF the Packet sending the packet is being watched then the packet is decoded into decoded ID and is compared with plain text ID, if the watcher and forwarder node can't find the key with success, they will try as many keys as the value of Virtual key search threshold before declaring the packet as malicious. If the packet is Authentic and this hop is not the Final Destination, the Original Packet Is forwarded else the node is bridging the VEBEK network. In case of Bridging original packet is encoded again with virtual bridge energy and forwarded. Both virtual and perceived energy from it are decremented as per reflected. And If the Packet is illegal according to rules made by the energy values within the virtual key search threshold window, it would be discarded. This continuous till the packet reaches the sink. VEBEK-II has more operations in it, as there stand a possibility of malicious code escaping from watcher and reaching sink, however unlike VEBEK-I the number of processing steps in VEBEK-II are less as less re-encoding is performed and decoding is not done at every end. Note that here the malicious packet may travel several hope before getting dropped, and that re-encoding is only done when the forwarding nod is bridging the network.

## 5. Conclusion

Communication is the Process that requires high level of security, integrity and authenticity of data and especially when this is talking place in WSN in really becomes expensive and difficult to implement. To keep these things in check we presented a secure communication framework called VEBEK for Wireless Sensor Networks.

IIN comparison to Other Key Management VEBEK has the Following Benefits: 1) It is less Chatty so it saves energy and is harder to detect by attackers. 2) It uses Dynamic Way To generate key thus making it more efficient against various attacks (eg. Replay attacks, brute force attacks and masquerade attacks) and 3) It Provides A flexible Architecture to vary the level of security from high to low as per the requirement of the task. 4) The energy and the cost saving by the VEBEK also Decrease by around 60 to 90 percent improvement. We have seen that **VEBEK (I and II)** are very efficient network of communication for WSN and if the wireless sensors are the technology of the Future then VEBEK is the way to bring it to reality.

## 6. References

[1]. 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.

[2]. Analysis of Public-Key Cryptography for
Wireless Sensor Networks Security F. Amin, A. H. Jahangir, and H. Rasifard.