"Dynamic encryption for Wireless Sensor Network using RC4 Algorithm"

[1] Ch .Devasena
E&C Dept.,
YDIT, Bangalore, India.
[1]ch_devasena@yahoo.co.in ,

[2]Veeresh Patil
E&C Dept.,
YDIT, Bangalore, India.
[2] veeresh91@yahoo.co.in ,

[3]Lokesh.L
E&C Dept.,
YDIT, Bangalore, India.
[3]lokeshadithya9@gmail.com

***ABSTRACT*: Since Energy is the important resource of wireless sensor network (WSN) node, a secure, dynamic encryption algorithm has introduced for wireless sensor networks which eliminates redundant sensor, reduces the energy and the cost of communication even in aggressive environment. This framework is the virtual energy Based Encryption and keying technique called "VEBEK". It uses the idea of sharing a dynamic virtual energy among the sensor nodes. It uses simple encryption algorithms i.e. RC4 encryption mechanism. The key to the RC4 encryption is a dynamic key which is the real time behavior of the residual virtual energy of the node at that instant. Therefore each packet will have a separate dynamic key. This framework has two modes of operation:VEBEK-1 & VEBEK-2. In VEBEK-1 each node watches its one hop neighbors.Whereas in VEBEK-2 Nodes are configured to watch some of the nodes in the network.**

Keywords: Virtual energy based Encryption and keying, Dynamic cryptic credentials, security.

I.INTRODUCTION

The Wireless Sensor Network is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors[1]. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors which will monitor physical or environmental conditions. The most relevant applications are Event detection, periodic measurements, function approximation and edge detection, Tracking. In many applications individual nodes in the network have to rely on onboard batteries, limited supply of energy. Wireless sensor nodes have existed for decades and their development was motivated by military applications such as battlefield surveillance. The boom of a wireless sensor technology became their use in most of the fields like environmental, industrial, military etc. and it may become in future to use sensors in our day to day life.

The employed architecture and protocols for WSN must support long life times[3]. Achieving this task efficiently requires energy –efficient routing protocol to set up paths between sensor nodes and the data sink. Security requirements of WSN impose costly constraints and overhead due to a sensor node's limited power supply and computational resources. 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.

Hence the protocols designed have to utilize limited resources efficiently for the sensors thus the resource usage on field has to be most efficient. In this paper we focus on communication of information by providing security, authenticity and integrity. .

Therefore we present a Flexible modular framework for WSN applications using virtual energy and simple encryption algorithm. In this paper we primarily focus on the keying mechanism based on two fundamental schemes for wireless sensor networks. They are Static and Dynamic key management schemes. In static, the key Management functions (key generation and distribution) are carried prior to or shortly after network attack resilient than static ones. But they have a major disadvantage of more communication cost due to keys being refreshed to update the keys, to remove stale keys in the network.

ORGANIZATION:

This paper is organized in the following sections.Section II describes the Background of framework.Section III describes Block diaram of VEBEK structure. Modes of operation in section IV. Result and performance analysis in section V. In Section VI conclusion and future work are given.

II.BACKGROUND OF FRAMEWORK:

Efficient key management schemes: Static or dynamic are used to provide important aspect of confidentiality[5]. Keys are provided before deployment of the network(Static key scheme) or redistributed to

the nodes as and when triggered by keying events(Dynamic key scheme).

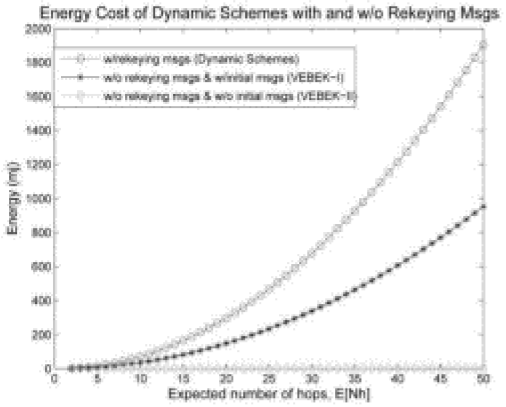

Fig 1: *Energy consumption for Keying in Dynamic Energy based schemes (VEBEK-I and VEBEK-II).*

In our framework we use Dynamic Keying scheme without many control messages for rekeying so that we can maintain the health of the network security and can reduce the energy cost function. The energy consumption based on Dynamic keying schemes are compared for two operational modes of VEBEK framework.

With this we can analyze Dynamic key based schemes consume more energy for exchanging rekeying messages. Whereas VEBEK framework consumes energy for generating the keys and protection of information. It does not exchange messages for key renewal.

III .VEBEK FRAMEWORK:

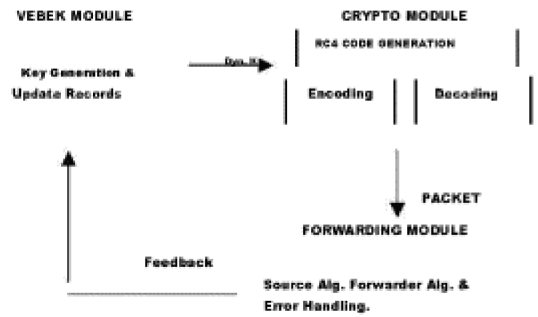

Fig 2: Vebek structure

The above fig. shows the VEBEK framework. It has three modules. Virtual Energy Based Keying module, Crypto module and Forwarding module which arediscussed below in detail. The same type of structure will be there at each node.

A. Virtual Energy Based Keying Module:

The Virtual Energy Based Keying Module is used for handling the keying process. It generates a dynamic key which is then given to the crypto module, which is the function of virtual energy of that particular node at that instant[7]. In reality battery levels may vary and the differences in battery levels across nodes cause packet dropping.

When the sensor network is active nodes traverse different functional states such as node-stay-alive,packet transmission, packet reception, encoding and decoding. As each of these states occur, the virtual energy of the node reduces largely and the current value of the virtual energy Evc of the node at that instant is used as the key to the key generation function.

As we know each node performs some of the functional states given above and calculates, updates the transient virtual energy. Each state is associated with some energy. These energy values of different states are listed below.

Table 1: Notations used in VEBEK.

Etx	Tx energy	Esa	Stay alive energy
Erx	Rx energy	Evc	Virtual c st
Eenc	Encoding energy	Ep	Perceive d energy
Edec	Decoding energy	Efw	Forwarding energy
Ecomp	Computational energy	Edyn	Dynamic keying cost
N	# of nodes	R	# of watched nodes

Flowchart to compute Dynamic Key:

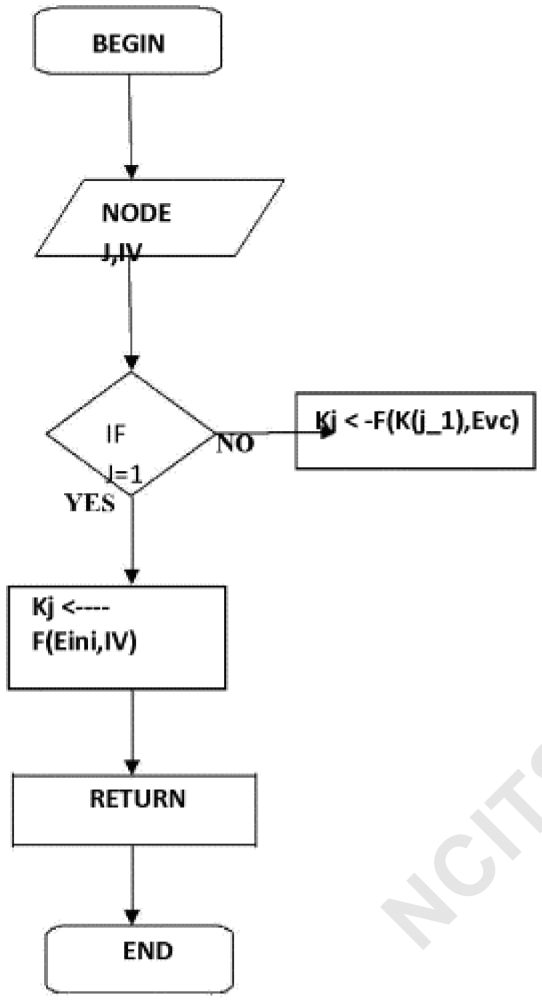

Fig 3: *Flowchart*

B. Crypto Module:

In our framework we use an Encryption mechanism which is simple and effective enough to make use of less energy. Basically it is a process of permutation of the bits in the packet in accordance with the permutation code which is generated by

RC4 encryption mechanism.

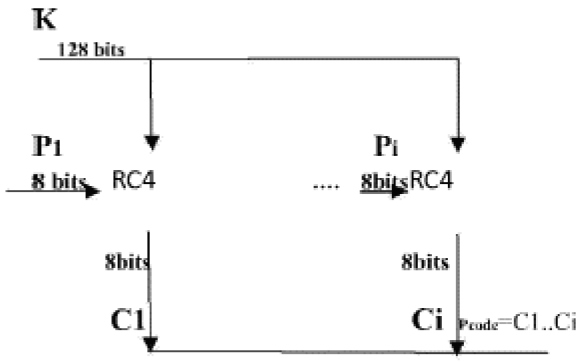

Fig 4: *RC4 Encryption Mechanism.*

The packets in VEBEK consists of the ID (i-bits), type (t-bits) (assuming each node has a type identifier), and data (d-bits) fields. Each node sends these to its next hop. The permutation code used to encode the

[ID/type/data] or X message. An additional copy of the ID is also transmitted in the clear along with the encoded message. The final packet is in the form of [ID{Id/type/data}k]. Where {x}k is the encoding X with key k.

C. Forwarding Module:

It is the final module of VEBEK framework. Its job is to send the packets commenced at the source node or to receive packets from forwarding nodes.

C.1 Source Node Algorithm

The event detected by a source node is to be secured. After generation of dynamic key by VEBEK module the key is used as input to the RC4 algorithm within the crypto module which generates a permutation code for encoding the message. This encoded message and clear text ID of the originating node are transmitted to the next node. The local virtual energy value is updated and stored for use with the transmission of the next report.

C.2 Forwarding Node Algorithm:

The forwarding node receives the packet and check its watch list. to determine whether the packet came from the node it is watching . If the current node(forwarding node) is watching the node from which packet has arrived , then the current node checks the current virtual energy of the sending node and extracts the energy value to derive the key. It authenticates the message by Decoding it and comparing the plaintext node ID with the encoded node ID. If the node is not being watched by the current node ,the packet is forwarded

without modification or authentication.

IV. MODES OF VEBEK OPERATION:

The VEBEK framework has two modes of operation VEBEK-I and VEBEKII,

A. VEBEK-I:

IN VEBEK-I All nodes watch their neighbors. Packet received from a neighbor is decoded to verify its authenticity. Only tested packets are forwarded towards the sink. The illegal packets that are infected by malicious nodes are filtered in line.

B. VEBEK-II:

In the VEBEK-II nodes are configured to watch only some nodes in the network. In this if the current node is not watching the node from which packet has come it simply forwards the packet. If the current node is watching the node from which the packet has come, then the packet is decoded and the plaintext ID is compared with the decoded ID. If the key is not found by watcher and watching node, the packet is declared as malicious after giving number of trails using as many keys as the value of Virtual key search threshold.

V RESULTS AND PERFORMANCE ANALYSIS

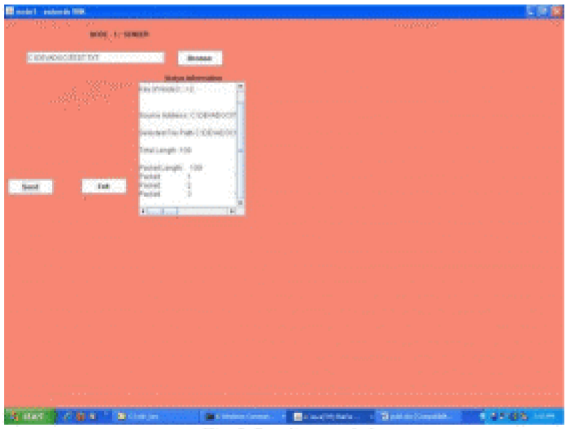

Fig 5:Sending node1

This node 1 is a sender shown in fig 5which after collecting data generates dynamic key and transmits information when we give send.

Depending upon VEBEK1,VEBEK2 forwarding node will perform Encoding,Decoding and Key generation operations.

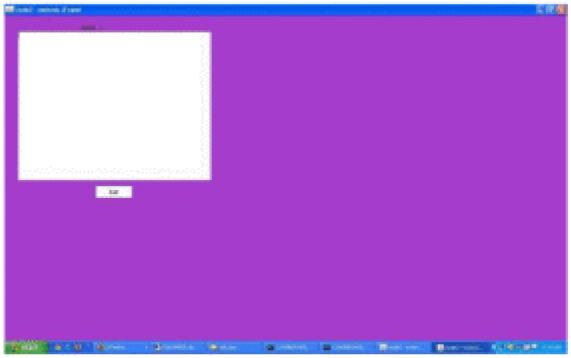

Fig 6:Forwarding node2

This is a destination node as shown in fig 6 which will receive original information from sender node1. The data received will be in terms of packets.

The table below shows the performance analysis of VEBEK.

Table 2:process of VEBEK modes of operation

	VEBEK-1	VEBEK-2
Node 1 Source node	Dynamic key,encoding	Dynamic key,encoding.
Node 2 Forwarder	Dynamic key,encoding,decoding.	Dynamic key,decoding if the node is in watchin list,encoding if the node is bridging the n/w.
Node 3 Forwarder	Dynamic key,encoding,decoding.	Dynamic key,decoding if the node is in watchin list,encoding if the node is bridging the n/w.
Node 4 destination	Dynamickey,decoding.	Dynamic key,encoding and decoding

VI. CONLUSION

By using VEBEK modular structure we can save energy ,cost as well as we can reduce the number of messages needed for rekeying in key management schemes.It is true that communication of any information must be secured,authenticated and integrated . Since communication cost is very high for certain wireless sensor network applications secured communication with a considerably less cost is a challenging problem. To keep these things in check we presented a flexible modular framework using VEBEK.

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. 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.

[3] S. Uluagac, C. Lee, R. Beyah, and J. Copeland, "Designing Secure Protocols for Wireless Sensor Networks," Wireless Algorithms, Systems, and Applications, vol. 5258, pp. 503-514, Springer, 2008.

[4] Crosshow Technology, http://www.xbow.com, 2008.

[5] H. Hou, C. Corbett, Y. Li, and R. Beyah, "Dynamic Energy-Based Encoding and Filtering in Sensor Networks," Proc. IEEE Military Comm. Conf. (MILCOM '07), Oct. 2007.

[6] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security, pp. 41-4, 2002.

[7] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," Proc. ACM MobiCom, pp. 56-67, Aug. 2002.

[8] Georgia Tech Sensor Network Simulator (GTSNetS),http://www.ece.gatech.edu/research/labs/ MANIACS/GTNetS, 2007.

[9] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.