International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Authentication in Wireless Sensor Networks Using Dynamic Keying Technique

Thiruppathy Kesavan Venkatasamy[1]* **Radhakrishnan Shanmugasundaram[2]**

[1]*Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India*
[2]*Kalasalingam University, Krishnankoil, Tamil Nadu, India*
*Corresponding author's Email: kesavanvt@mits.ac.in

Abstract: In this paper, Cluster Based Dynamic Keying Technique for Authentication in Wireless Sensor Networks (WSN) is proposed. The CH enabled by Global Positioning System (GPS) determines a Combined Cost Value (CCV) for each sensor node based on nodes location, node degree and virtual battery power. Since the key to the encryption scheme changes dynamically when there is change in CCV, separate dynamic keys are generated in each cluster by each CH and using RC5 encryption mechanism the source CH forwarding the data along different clusters along the path to the sink are able to verify the authenticity. When the source CH needs to transmit the aggregated data packet to the sink, it splits the packet into shares by threshold secret sharing algorithm and forwards them to the sink using multi-path dispersal routing technique.

Keywords: Clustering; Authentication; Multipath routing; Cluster; WSN.

1. Introduction

1.1. Heterogeneous Wireless Sensor Network

Wireless Sensor Networks (WSNs) are termed as tiny, low cost and low powered sensor nodes that dynamically construct the network in ad-hoc manner. Generally, WSN is formed of identical or dissimilar sensors. With the help of low level flying aircraft, the sensor nodes are organized around the pre-defined location [1, 2, 3, 4, 5].

H-WSNs can be utilized for various real time applications and can be operated in diverse environments [3, 6]. Every sensor possesses similar potentiality in terms of sensing and transmission range, battery power and processing power in case of homogeneous WSN. Whereas in H-WSN, there is an improvement in the network performance in the presence of high potential sensors with a better sensing range and transmission ranges [1].

1.2. Security Threats in WSN

Providing security in WSNs is a challenge due to the resource constraints in sensor nodes, the size and density of the networks. Since the sensor nodes are deployed in unattended area, providing physical security is also impossible. The topology cannot be predicted before the deployment due to the nature of wireless communications. Data confidentiality, integrity, authenticity and availability are considered as the security requirements. These requirements must be satisfied by WSN even in the presence of powerful attackers. [7, 8, 9]

1.3. Keying in WSN

In WSNs, the message encryption mechanism helps in realizing the secure wireless communications. Many nodes in the network share a secret encryption key, which is termed as session key [10]. The three simplest keying models such as network keying, pair-wise keying and group-wise keying can be used to compare the relationship among the WSN security and its operational needs [7]. Scalability and flexibility are the major advantages of network keying model. Handling the single key allows easy coordination among the nodes in the network. However, the major drawback is, if an attacker, he can, compromises a single node or the key simply compromise the whole network [7, 11, 12].

1.4. Bootstrapping

Bootstrapping [6] is a process to be executed by every sensor node once it is deployed in the field. While deployment, the sensor nodes do not have any direct contact with each other. Before deployment, the sensor nodes have to be initialized with some secret information. This secret information can be used during bootstrapping to get coordinated among them.

1.5. Authentication

Authentication is one of the security requirements that verify the identity of a sensor node. In sensor networks, generally the routing messages are broadcasted in the network; especially the advertisement messages. If authenticity is not included in those messages, any compromised node can claim as legitimate node and it would be so hard to identify the compromised node [13].

1.6. Energy and Power

Among various methods available in cryptography, the public key cryptography consumes more power due to its complex encryption and decryption operation that uses modular multiplications [2, 8]. When the network topology is formed, the route setup process in WSNs is dependent on the consideration of the energy. As the reduced energy consumption of the wireless link is proportional to square or even higher order of the distance between the sender and receiver, it is assumed that multi-hop routing utilizes minimum energy than direct communication [14]

1.7. Problem Identification

The transmission power for communication between nodes is a monotonically increasing function of the distance. Under the assumption that routing is optimally selected to minimize the total transmission power, nodes that are physically close have overlapping routing paths and will have common links in the path from the CH towards them. Hence, they should also share common keys in order to receive the same key updates and reduce the energy expenditure of the key distribution. We propose a cluster-based design approach for key estimation that consists of location of the nodes node degree and virtual battery power to reduce the energy expenditure of the key distribution.

The rest of the paper is arranged as follows: a concise account of certain literary works in Section 2, a description of proposed method illustrated in Section 3. The test outcomes and relative analysis debate are offered in Section 4. At last, the conclusions are furnished in Section

2. Related Work

C. M. Yu et al [15] have proposed a Constrained Random Perturbation-based pairwise key establishment (CARPY) scheme for WSNs. This scheme provides resilience to dynamic environments along with guaranteed key establishment and efficiency. CARPY was an improved version of Blom's concept, which consist of two steps: off-line step and the on-line step.

R. Lu et al [16] have proposed a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data. It detects and filters the false injected data by using the random graph characteristics of sensor node deployment and the cooperative bit-compressed authentication technique.

B. Kadri et al [17] have proposed a lightweight implementation of public key infrastructure called cluster based public infrastructure (CBPKI). In CBPKI, to ensure data confidentiality and integrity, session keys were established between the base station and sensors by executing a set of handshakes. Regarding the security services, it seems that CBPKI ensure all security services and it is robust against several attacks with low power consumption and network overhead.

J. Kim et al [18] have proposed an efficient and scalable re-authentication protocol over wireless sensor network. They have used an efficient method of membership verification for re-authentication of mobile nodes. In addition, they provided performance and security analysis of their protocol.

Z. Yu and Y. Guan [19] have proposed a novel key management scheme using deployment knowledge. In this scheme, a target field was divided into hexagon grids and sensor nodes are grouped and deployed into each into a unique grid. By using deployment knowledge, they have significantly reduced the number of potential groups from which a node's neighbors may come.

X. Du et al [20] have designed an ECC based key management scheme for heterogeneous sensor networks along with the topology changes due to node failures. When the data generated by neighbor nodes are highly correlated, Minimum Spanning Tree (MST) was used for routing; otherwise, Shortest Path Tree (SPT) was used.

Arif et al [21] have proposed a secure communication protocol called Virtual Energy-Based Encryption and Keying (VEBEK) scheme for WSNs. This protocol avoids exchanging of

messages to dynamically change its key. The keys were updated as a function of residual virtual energy of the sensor node. In VEBEK, since all the nodes are maintaining the watch list, the transceiver should be always active in order to watch the transactions of their neighboring nodes and hence the energy is wasted.

S. Banihashemian and A. G. Bafghi [22] proposed a key management scheme for heterogeneous sensor networks that provides higher connectivity and resiliency. In their concept, they have used the distance from the cluster head which was obtained during clustering phase. New keys were derived from different seeds for different level.

V. Thiruppathy Kesavan and Radhakrishnan [23] have proposed a Cluster Based Dynamic Keying Technique (CBDKT) for authentication in wireless sensor networks. The Cluster Head (CH) determines a Combined Cost Value (CCV) for each sensor node based on node location, node degree and residual battery power. Since the key to the encryption scheme changes dynamically when there is a change in CCV, the CH generates separate dynamic keys in each cluster.

3. Secure Cluster Based Multipath Routing

3.1. Overview

In this paper, a Cluster Based Dynamic Keying Technique for WSN is proposed. Initially the nodes are grouped into various clusters according to distance. A CH is elected which is GPS enabled. With the help of CH, all the cluster members can estimate their locations. Each cluster member also estimates its node degree by calculating its neighbors. The CH has a member table, which contains the details of each member ID, its location, node degree and virtual battery power to send one packet to the CH. Then the CH determines a CCV for each sensor node based on these parameters. This CCV is also maintained in the member table. The key to the encryption scheme dynamically changes as a function of the CCV of the sensor, thus requiring no need for re-keying.

3.2. Cluster Formation

The CH forwards a hello packet to all available sensor nodes for reporting its location. This is performed with the help of non-persistent Carrier Sense Multiple Access (CSMA) MAC protocol that includes the maximum transmit power (p_m) of a sensor node similar to LEACH concept [24]. The sensor nodes far away from the CH utilize intermediate nodes to convey their data through multihop communication owing to short transmission ranges of sensor nodes. This is because the node away from the CH consumes more energy in comparison to the nodes close to the CH.

The non-CH node upon receiving hello packets comes to know to which cluster it belongs. This is performed by comparing the Received Signal Strength (RSS) from all neighboring CHs. The non-CH node finds the minimum hop distance (HD_{min}) [25] between itself and its corresponding CH with the help of received power (p_r) from the CH and transmission range of the sensor nodes (n_t).

$$HD_{min} = \acute{\varepsilon} \sqrt{\frac{(p_m / p_r)}{n_t}} \quad (1)$$

Where, p_m is the maximum transmit power and $\acute{\varepsilon}$ denotes the path-loss exponent.

3.3. Location estimation

Each sensor node evaluates the location probability [26] as per following equation

$$\rho = \frac{Dist.between\ estimated\ location\ and\ CH}{rectification\ factor} \quad (2)$$

While discovering the location of CH, measurement for Euclidian distance of one hop is estimated and it is referred as rectification factor.

Using the value of ρ, and the actual hop count, the probability P_{ij} is calculated as per following equation:

$$P_{ij} = \frac{\rho^{\mu-1} e^{-\rho}}{(\mu-1)!.} \quad (3)$$

In the above equation, μ denotes the number of hops (μ=1, 2...) and ρ represents the distance between CH and location that is being measured.

3.4. Virtual Battery Power

In this work, Virtual Battery Power (V_{BP}) is considered instead of the real battery power because the differences in the power ranges across the nodes which induce synchronization issues that result in packet drops [21]. It is assumed that each sensor node possess certain V_{BP} when it is initially deployed.

The sensor nodes pass through several functional states such as node-stay-alive, packet reception, transmission, encoding and decoding after deployment. During these states, the sensor node will forward either some other sensor's data or injecting its own data into the network. Thus based

on the actions performed by the node, the associated power are as follows.

P_{rx}- reception power
P_{tx} - transmission power
P_{enc}- encoding power
P_{dec}- decoding power
P_a - power required to maintain the node in the alive state.
P_{sync}- power utilized to synchronize the source
P_{MAC} – power required to generate MAC code
P_{auth} –power required for authentication

When a source node detects any event, it forwards the packet size (β) towards the sink. The virtual cost (V_{cs}) related to this source node is computed using the following equation:

$$V_{cs} = \beta(P_{tx} + P_{enc} + P_{MAC}) + tP_a + P_{SYNC} \quad (4)$$

Where β = packet size
t = duration of alive state of the node.

When any CH receives the data from any node, the V_{BP} can be updated by decrementing the cost associated with the actions performed by the sender. The Virtual Cost (V_{ci}) related to the intermediate node is computed using the following equation.

$$V_{ci} = \beta(P_{rx} + P_{auth} + P_{dec} + P_{tx} + P_{enc}) + 2tP_a \quad (5)$$

Thus, the transient value of the V_{BP} is obtained by decrementing the pre-defined virtual cost (V_c) from the previous V_{BP}, which is represented using the following equation.

$$V_{BP} = P_i - V_c \quad (6)$$

Where P_i = previous V_{BP}

After every action, each node computes and updates the transient value of the virtual energy.

3.5. Cost computation

CH constitutes the member table that includes the details of each member id, its location, node degree and virtual battery power. Then the CH determines a CCV for each sensor node based on these parameters. This CCV is also maintained in the member table.

Each Node Location (NL) is given by the (x, y) coordinates and is computed as per (section 3.3). The Node Degree (ND) is estimated based on the neighboring nodes information. As location and node degree of a node are constant for a static network, both NL and ND values remain static. The V_{BP} is dynamic in nature since it varies depending on the node state. The computation of cost function is as follows:

$$CCV = \dot{\alpha}(x_a + y_b) + \beta ND + \gamma V_{BP}(c) \quad (7)$$

Where ά, β and γ are normalization factors and

a and b are constants (assigned during runtime)

Every time the V_{BP} is decremented, the cost function is updated.

3.6. Dynamic Key Generation

In sensor networks, sensor node traverses through the several functional states. The functional states may include

- Active state of the node
- Reception and transmission of packet,
- Encoding and decoding phases.

Each sensor node has V_{BP} during its initial deployment in the network. During the above functional states, there may be depletion of V_{BP} in the sensor node.

Let V_{BPc} = current value of the virtual battery power

F_k= key generation function.
C_i = initial cost of the sensor node.
C_k= current cost value updated by R_c
k_i = initial key.
V_i = initialization vector.

The node's V_{BPc} is used as the key to F_k. When the sensors are initially deployed, they contain C_i and hence k_i is the function of the C_i and V_i .i.e. $k_i = f(C_i, V_i)$. V_i values are distributed to the sensors. Consequently $k_j = f(C_k, K_{j-1})$. Here k_{j-1} represents the previous value of key.

Every detected packet is related with a new unique key which is generated based on the transient values of the V_{BP} and the keying module assures this aspect. The key generation scheme is initiated whenever data is sensed and hence no separate methodology is required to update the keys.

The condition for computing the dynamic key is as follows:

At start, i ← t , [t ←ID of plaintext]

If i = 1
Then
$K_j \leftarrow f(C_i, V_i)$
Else
$K_j \leftarrow f(K_{j-1}, C_k)$
End if

3.7. Encoding Scheme

The purpose of encoding scheme is to offer simple confidentiality of the packet header and payload while ensuring the authenticity and integrity of sensed data without incurring transmission overhead. The encoding mechanism refers to the

process of permutation of bits in the packet according to the dynamically created permutation code through the RC5 encryption mechanism [27]. The key to RC5 is generated with the dynamic key generation module as per section 3.6.

Finally, the packet to be forwarded will be with the field that includes [*ID {k(z)}*] and *k(z)* constitutes the message z encoded by key k. Instead of forwarding the hash value along with the information to be forwarded, in this scheme the result of the permutation code value is used locally. When the next cluster along the path to sink receives the packet, it generates the local permutation code to decode the packet.

After the event detection, the source node needs to maintain the secured reports and it utilizes the $V_{BP}(c)$ and V_i to construct the next key as per section 3.6. Further, the key is given as input to the RC5 algorithm inside the encoding module to generate a permutation code for encoding the [z] message.

3.8. Authentication Technique

The node computes the message authenticity and integrity code (MAC) which offers hash function over the encoded message and destination address and this message is forwarded to the CH.

The message forwarded to the CH will be in the following format.

$$MAC\left[ID\left\{C_p(z)\right\}\right] = H\left[ID\left\{C_p(z) \,||\, Ad_d\right\}\right] \qquad (8)$$

Where ID is the identity of the originating node

$C_p(z)$ constitutes the encoding data with permutation code C_p.

Ad_d represents the destination address of the CH.

When the CH receives the message, it checks for the associated $V_{BP}(c)$ stored in the sending node. Then it extracts $V_{BP}(c)$ to estimate CCV and derives the dynamic key k[z]. The CH then computes the MAC over the received message using k[z] with sensor node that is represented as MAC_{ch}.

On comparison, if MAC and MAC_{ch} are found to be similar, the message is to be authenticated. The authenticated message is then decoded by the CH using the same key k[z] and forwarded to the neighboring CH. If authentication fails, the message is considered as unauthenticated and returned to the node itself [28].

4. Multi-path Dispersal Routing

4.1. Dispersal Technique

When the CH needs to transmit the aggregated data packet to the sink, it splits the packet into q shares according to *(t, q)* – threshold secret sharing algorithm. e.g. Shamir's algorithm [29]. The application of this scheme is concerned with the cooperation of group of mutually suspicious individuals with incompatible interests. The useful properties of this module are

- The size of the shares does not exceed the size of the original data.
- When the *t* is kept fixed, shares can be dynamically added or deleted without affecting the other shares.

The multi-path dispersal routing is used to transmit the shares to the next CH. Each share holds a TTL field and the source node assigns the initial value of Time To Live (TTL) field for controlling the total number of random transmission. The value of TTL field is reduced by one after each transmission. After the TTL field reaches zero, the last CH to receive the shares begins its transmission towards the sink. When the sink gathers minimum of *t* shares, it can rebuild the original packet.

4.2. Multi-path Routing

Multi-path routing [30] is established for transmission of q shares from CH to the sink. The multi-path routing protocol usually desires the node-disjoint paths owing to use of most accessible network resources. In order to perform the route discovery, we consider the following phases

Phase 1: Initialization Phase Every CH broadcasts a HELLO message through the network to contain enough information regarding its nearest neighbors. The HELLO message includes the information such as source ID, hop count and V_{BP} that is given in table 1. In this phase, CH maintains and updates a buffer table that includes the information about the list of the neighbor CHs.

Table 1. Format of Hello message

Source ID	Hop count	Virtual battery power	Free buffer

Phase 2: Route Discovery Phase After phase 1, sufficient information is available in every CH for computation of cost function for its neighboring CHs. The source CH(CH_s) computes the preferred next hop CH. Then it broadcasts the Route REQuest (RREQ) message to the chosen next hop CH that is shown in Figure 1. The RREQ message includes the source ID, destination ID, cluster ID, and V_{BP}(As per table 2). Likewise, the next hop CH of the source CH, computes its most preferred next hop in the sink

node's direction and the process continues until the RREQ message reaches the sink node.

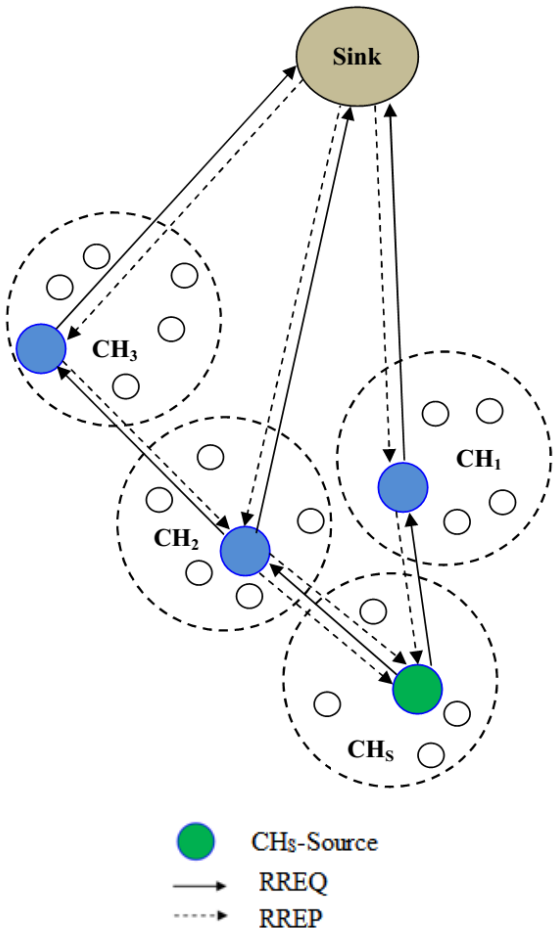

Figure.1 Route Discovery

Table 2. Format of RREQ message

Source ID	Destination ID	Cluster ID	Virtual battery power	Free buffer

After reception of all RREQ message, the sink node replies back CH_s with the Route REPly (RREP) message via the path traversed by the RREQ messages. Based on the RREP, CH_s discovers the available paths and forward s*q* shares through these paths towards the sink node.

The above process of multipath dispersal routing from CH to the sink is described using the figure 2. The paths established as follows.

Path 1:$CH_s \rightarrow CH_1 \rightarrow$ Sink

Path 2: $CH_s \rightarrow CH2 \rightarrow$ Sink

Path 3: $CH_s \rightarrow CH_2 \rightarrow CH_3 \rightarrow$ Sink

Through the selected paths, the CH_s forward the shares towards the sink node.

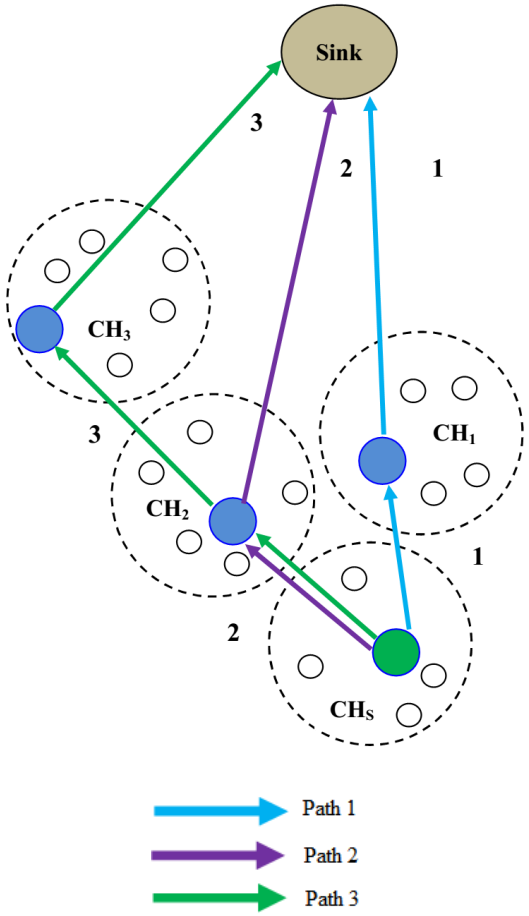

Figure.2 Multi-Path Dispersal Routing

5. Overall Algorithm of the Proposed Approach

The entire steps involved in the proposed technique are summarized in the following algorithm.

Step 1: The nodes are grouped into various clusters in terms of distance. For each cluster, a CH is chosen.

Step 2: Every node estimates their location with the help of CH, node degree by calculating its neighbors, and V_{BP} as per energy redeployment set.

Step 3: CH computes the CCV for each sensor node based on the estimated location, node degree and V_{BP}.

Step 4: Each CH generates the dynamic keys separately in each cluster as a function of combined cost value of the sensor.

Step 5: Using RC5 encryption scheme, the data packets are encoded by the sender with the dynamic key.

Step 6: The sender node computes MAC code that provides the hash function over the encoded

message and destination address and this message is forwarded to its CH.

Step 7: When CH receives the message, it checks for the associated virtual battery power stored in the sending node. Then it extracts V_{BP} to estimate CCV and derives the dynamic key.

Step 8: CH computes the MAC over the received message using the derived dynamic key with sensor node.

Step 9:

If MAC generated at the node ≈ MAC generated at CH

Then

The message is considered as authenticated and this message is decoded by the CH using the same dynamic key and forwarded to the neighboring CH**.**

Else

The message is unauthenticated and returned to the node itself.

End if

Step 10: CH repeats the process of MAC computation for every received packet from its member nodes to verify whether it is authenticated.

Step 11: CH aggregates the entire data received from the source and split into n shares as per threshold secret sharing algorithm and then forwards them towards the sink through multi-path dispersion technique.

Advantages of this Approach

1) Since the keys to the encryption scheme are dynamic in nature, the approach is resistant to node capture attacks.
2) If any cluster member becomes an attacker, the confidentiality of forwarded data will not be affected. This is because every node encrypts the data with a dynamic key and then sends it to the CH in a secured way.
3) If any CH becomes an attacker, any misbehaving action will not affect the data, since it can access only a portion of data. Also, the sink node can reconstruct the data after reception of sufficient shares.
4) Since it involves less key updating operations, energy cost associated with keying is reduced.
5) Even if the sensor node becomes mobile, this technique can be applied since nodes location and node degree are taken into consideration while computing key cost function.

6. Simulation Results

The proposed Combined Cost Based Dynamic Keying Technique (CCBDKT) is evaluated using NS-2 [31] simulation. A random network of sensor nodes deployed in an area of 500 X 500m is considered. The sink node is assumed to be situated 100 meters away from the above-specified area. The simulated traffic is CBR with UDP with the rate of 256 kbps. Different energy levels 30 Joules and 20 Joules were assigned for CH and the member nodes respectively. The number of clusters formed is 9. Out of which, the data is transmitted from 4CHs to the sink. 3 sensor nodes in each cluster are sending data to their CH. The numbers of attackers vary from 1 to 5.

To calculate the values of the normalization constants $\acute{\alpha}$, β and γ, their values are considered between 0 and 1 such that $\acute{\alpha} + \beta + \gamma = 1$. Initially the value of $\acute{\alpha}$ as 0.2, β as 0.2 and γ as 0.6 is taken.

In initial experiment, the number of attackers vary from 1 to 5 from various clusters performing black hole and packet dropping attacks. The number of nodes in the network is fixed as 100.The performance of CCBDKT is compared with the VEBEK - II [21] scheme.

(i) Packet Drop Ratio

It is given by the ratio of packet dropped to the total packets sent.

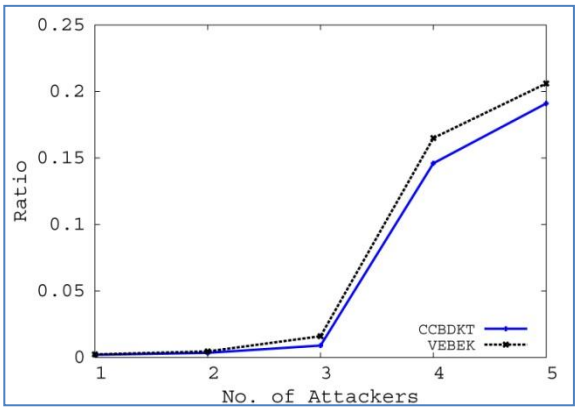

Figure.3 Average Packet Drop Ratio

Figure 3 shows the average packet drop ratio of both the schemes. When the number of attackers is increased, the percentage of packet drop is increased and hence the drop ratio is increasing. However, CCBDKT has shown reduced packet drop ratio, when compared to VEBEK. This is because of the fact that CCBDKT uses the multi-path dispersion technique, which mitigates the effect the attackers.

(ii) Energy Consumption

The average energy consumed for the data transactions is measured in Joules.

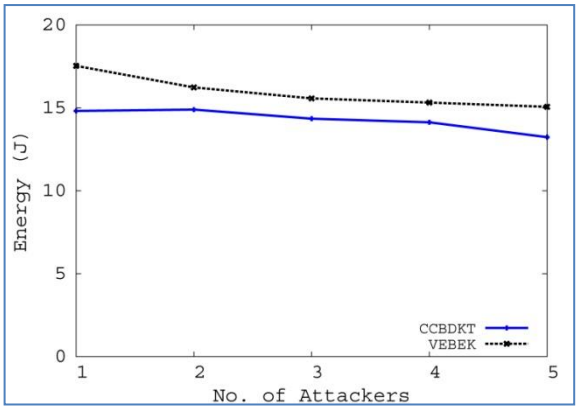

Figure.4 Average energy consumption in the network

Figure 4 shows the average energy consumption of both the schemes. From the figure, it is seen that the average energy consumption decreases, when the numbers of attackers are increased. This is due to the reason that the percentage of correctly received data traffic reduces as the number of bad packets increases by the attackers in the network. When compared to VEBEK, CCBDKT has consumed less energy because of the cluster based routing approach. Due to the clustering based approach, the CH itself authenticates the packets received from its neighbors and hence, the energy consumption is less over the network. Due the energy heterogeneity of the CH, it does not affect the lifetime of the entire network. However, in VEBEK – II, the nodes are watching more than one neighbor's transactions where it consumes more energy in the network. In addition, more than one intermediate (watcher-forwarder) nodes towards the sink checks for the authenticity of the packets, the energy consumption is more in VEBEK – II.

(iii) Packet Delivery Ratio

Packet Delivery Ratio is the ratio of the number of packets received successfully and the total number of packets transmitted.

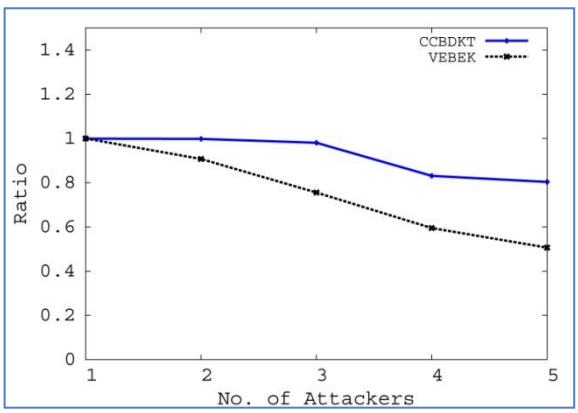

Figure.5 Packet Delivery Ratio

Figure 5 shows the packet delivery ratio of both the schemes. It is evident that when attackers are increased, the percentage of packet drop is increased and hence the packet delivery ratio is decreased.

(iv) Computation and Total Energy Cost

Dynamic keying schemes involve re-keying or key updating phase in order to renew the security of the nodes. Hence, the energy cost function for the keying process from a source sensor to the sink while sending a message on a particular path with dynamic key-based schemes is written as follows:

Energy Cost of VEBEK

In VEBEK, in both operational modes, the single cost (E_{So}) is the summation of stay-alive, sense the event, encode the packet, and transmit the packet (E_{sa}, E_{sens}, E_{enc}, E_{tx}) at the source sensor. Thus,

$$E_{So} = E_{sens} + E_{enc} + E_{tx} + E_{sa} \quad (9)$$

In VEBEK-II, the forwarding cost (E_{FW}) for all of the intermediate nodes is given by

$$E_{FW} = E_{rx} + E_{dec} + E_{enc} + E_{tx} + E_{sa} \quad (10)$$

Hence, the average cost to transmit a packet in VEBEK-II using (9) and (10) is

$$E_{av} = E_{So} + (E[_{nhw}]E_{FWw}) + (E[_{nhnw}]E_{FWhw}) \quad (11)$$

Where $E[_{nhw}]$ and $E[_{nhnw}]$ are given by expected number of hops along the path which are watcher and non watcher nodes, respectively.

Energy Cost of CCBDKT

E_{rx}- reception power
E_{tx} - transmission power
E_{enc}- encoding power
E_{dec}- decoding power
E_a - power required to maintain the node in the alive state.
E_{sync}- power utilized to synchronize the source
E_{MAC} – power required to generate MAC code
E_{auth} –power required for authentication

The associated cost at various functional states is given by the summation of node-stay-alive, packet reception, transmission, encoding costs.

$$E_{ASo} = E_{tx} + E_{enc} + E_{MAC} + E_a + E_{sync} \quad (12)$$

The forwarding cost is given by

$$E_{FW} = E_{rx} + E_{auth} + E_{dec} + E_{tx} + E_{enc} + E_a \quad (13)$$

Hence, the average cost to transmit a packet using (12) and (13) is

$$E_{av} = E_{ASo} + (D(E_{FW})) \quad (14)$$

Where, D is the distance between the source and the CH.

The computation cost associated with encoding, authentication and decoding is given as

$$E_{comp} = (E_{enc} + E_{MAC}) + (D(E_{auth} + E_{dec} + E_{enc})) \quad (15)$$

The computation and total energy cost of both VEBEK and CCBDKT are given in figure 6 and 7, respectively.

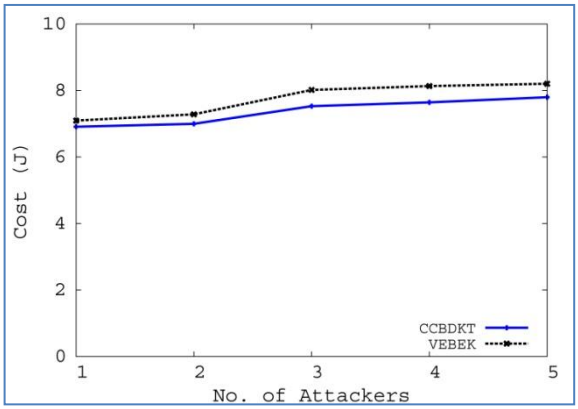

Figure. 6 Computation Cost

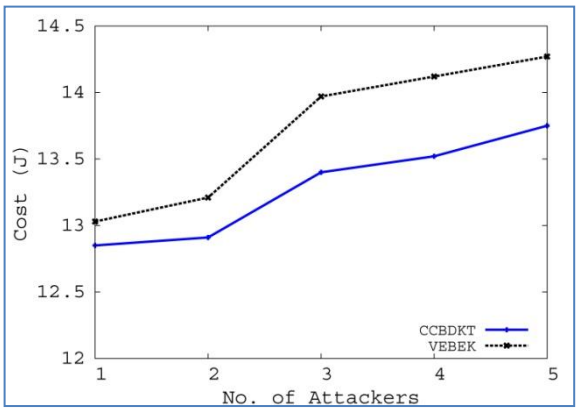

Figure.7 Total Energy Cost

Figures 6 and 7 depict the computation and energy cost involved in the process of the entire transmission between each pair of source and destinations. It is observed that the cost increases rapidly as the number of attackers increases, as more number of intermediate nodes are involved.

However, for CCBDKT, the computation cost is 5% less and total energy cost is 3% less, when compared to VEBEK, since CCBDKT uses less number of hops by using the cluster based approach.

7. Conclusion

In this paper, Cluster Based Dynamic Keying Technique for wireless sensor networks (WSN) have been proposed. The CH enabled by global positioning system (GPS) determines a combined cost value (CCV) for each sensor node based on nodes location, node degree and virtual battery power. This CCV is maintained in the member table. The key to the encryption scheme dynamically changes as a function of the combined cost value of the sensor, thus requiring no need for re-keying. Therefore, separate dynamic keys are generated in each cluster by each CH and by using the RC5 encryption mechanism, the source CH forwarding the data along different clusters along the path to the sink are able to verify the authenticity and integrity of the data and to provide non repudiation. When the source CH needs to transmit the aggregated data packet to the sink, it splits the packet into q shares according threshold secret sharing algorithm. The multi-path dispersal routing is used for transmission of shares towards the sink node. Since the node location and degree are considered for key cost this keying technique can be applied for mobile nodes also. Further, in future security can be enhanced by providing security for routing.

References

[1] Y. Wang, "Intrusion Detection in Gaussian Distributed Heterogeneous Wireless Sensor Networks", *In proceedings of IEEE Global Communication Conference (GLOBECOM)*, 2009.

[2] M. Qiu, C. Xue, Z. Shao, M. Liu, E. H. M. Sha, "Energy Minimization for Heterogeneous Wireless Sensor Network", *Journal of Embedded Computing - Design and Optimization for High Performance Embedded Systems archive*, Vol. 3, No. 2, pp. 109-117, 2009.

[3] J. M. Corchado, J. Bajo, D. I. Tapia and A. Abraham, "Using Heterogeneous Wireless Sensor Networks in a Tele monitoring System for Healthcare", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 14, No. 2, pp. 234-240, 2010.

[4] G. Wagenknecht, M. Anwander and T. Braun, "Demo: MARWIS - a Management Architecture for Heterogeneous Wireless Sensor Networks", *Wired/Wireless Internet Communications*, pp. 177-188, 2008.

[5] P. Antonio, F. Grimaccia and M. Mussetta, "Architecture and Methods for Innovative Heterogeneous Wireless Sensor Network Applications", *Remote Sensing*, Vol. 4, No. 5, pp. 1146-1161, 2012.

[6] K. Selvarajah, C. Shooter, L. Liotti, and A. Tully, "Heterogeneous wireless sensor network for transportation system applications", *International Journal of Vehicular Technology* , 2011.

[7] Z. S. Bojkovic, B. M. Bakmaz and M. R. Bakmaz, "Security Issues in Wireless Sensor Networks", *International Journal of Communications*, Vol. 2, No. 1, pp.40-40, 2008.

[8] W. Gu, N. Dutta, S. Chellappan and X. Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks", *IEEE Transactions On*

Network And Service Management, Vol. 8, No. 3, pp. 205-218, 2011.

[9] J. Zhang and V. Varadharajan, "A New Security Scheme for Wireless Sensor Networks", *IEEE Global Telecommunications Conference, (GLOBECOM)*, pp. 1-5, 2008.

[10] T. Landstra, S. Jagannathan and M. Zawodniok, "Energy-Efficient Hybrid Key Management Protocol for Wireless Sensor Networks", *International Journal of Network Security*, Vol. 9, No. 2, pp. 121-134, 2009.

[11] W. Du, J. Deng, Y. S. Han and P. K. Varshney, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks", *Journal ACM Transactions on Information and System Security (TISSEC)*, Vol. 8, No. 2, pp. 228-258, 2005.

[12] S. Ruj, A. Nayak and I. Stojmenovic, "Fully Secure Pairwise and Triple Key Distribution in Wireless Sensor Networks using Combinatorial Designs", *Proc: IEEE INFOCOM*, pp. 326-330, 2011.

[13] J. Kim, J. Lee and K. Rim, "Energy Efficient Key Management Protocol in Wireless Sensor Networks", *International Journal of Security and Its Applications*, Vol. 4, No. 2, pp. 1-12, 2010.

[14] L. T. Nguyen, X. Defago, R. Beuran and Y. Shinoda, "An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks", *IEEE International Symposium on Wireless Communication Systems, ISWCS*, pp. 568- 572, 2008.

[15] C. M. Yu, C. S. Lu and S. Y. Kuo, "Noninteractive Pairwise Key Establishment for Sensor Networks", *IEEE Transactions on Information Forensics and Security*, Vol. 5, No. 3, pp. 556-569, 2010.

[16] R. Lu, X. Lin, H. Zhu, X. Liang and X. Shen, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, No. 1, pp. 32-43 2012.

[17] B. Kadri, D. Moussaoui, M. Feham and A. Mhanned, "An Efficient Key Management Scheme for Hierarchical Wireless Sensor Networks", *Wireless Sensor Network*, Vol. 4, No. 6, pp. 155, 2012.

[18] J. Kim, J. Baek and T. Shon, "An Efficient and Scalable Re-authentication Protocol over Wireless Sensor Network", *IEEE Transaction on Consumer Electronics*, Vol. 57, No. 2, pp. 516-522, 2011.

[19] Z. Yu and Y. Guan, "A Key Management Scheme Using Deployment Knowledge for Wireless Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19, No. 10, pp. 1411-1425 2008.

[20] X. Du, M. Guizani, Y. Xiao and H. H. Chen, "A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", *IEEE Transactions on Wireless Communications*, Vol. 8, No. 3, 2009.

[21] A. S. Uluagac, R. A. Beyah, Y. Li and J. A. Copeland, "VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks", *IEEE Transactions on Mobile Computing*, Vol. 9, No. 7, pp. 994-1007, 2010.

[22] S. Banihashemian and A. G. Bafghi, "A new key management scheme in heterogeneous wireless sensor networks", *Proceedings of the 12th IEEE International conference on Advanced communication technology, ICACT'10*, Vol. 1, pp. 141-146.

[23] V. Thiruppathy Kesavan and S. Radhakrishnan, "Cluster Based Dynamic Keying Technique for Authentication in Wireless Sensor Networks", *Journal of Mobile Communication and Power Engineering*, Vol. 296, pp. 1-8, 2013.

[24] W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", *IEEE Transactions on wireless communications*, Vol. 1, No. 4, pp. 660-670, 2002.

[25] S. G. Quan and Y. Y. Kim, "Fast Data Aggregation Algorithm for Minimum Delay in Clustered Ubiquitous Sensor Networks", *International Conference on Convergence and Hybrid Information Technology*, pp. 327-333, 2008.

[26] R. Stoleru and J. A. Stankovic, "Probability Grid: A Location Estimation Scheme for Wireless Sensor Networks", *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, pp. 430-438, 2004.

[27] R. L. Rivest, "The RC5 Encryption Algorithm", *Proceedings of the Second International Workshop on Fast Software Encryption (FSE)*, Vol. 1008, pp. 86-96, 1995.

[28] A. Abduvaliev, S. Lee and Y. K. Lee, "Simple hash based message authentication scheme for wireless sensor networks", *9th International Symposium on Communications and Information Technology (ISCIT)*, pp. 982-986, 2009.

[29] A. Shamir, "How to share a secret", *Communications of the ACM (CACM)*", Vol. 22, No. 11, pp. 612-613, 1979.

[30] B. Yahya and J. B. Othman, "REER: Robust and Energy Efficient Multipath Routing Protocol for Wireless Sensor Networks", *Proc: IEEE GLOBECOM*, pp. 1-7, 2009.

[31] Network Simulator, http://www.isi.edu/nsnam/ns

[32] C. C. Chen, Y. N. Li and C. Y. Chang, "A Novel Range-Free Localization Scheme for Wireless Sensor Networks", *International journal on applications of graph theory in wireless ad hoc networks and sensor networks, (GRAPH-HOC)* Vol. 4, No. 2, pp. 1, 2012.