RESEARCH REVIEW JOURNALS
Volume-04
Issue-05
May-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

A Framework for Enhancement of Network Data Security Adopting Dynamic Key Management of WSN's Approach

*1Itfaq Ahmad Mir, 2Prof.G.M.Mir, 3Mudassir Makhdhoomi & 4Anwaar Ahmad Wani

*1Research Scholar, Department of Computer Application, Mewar University, Rajasthan, INDIA.
2Professor, College of Agri. Engineering, SKUAST, Kashmir, J&K, INDIA.
3Assistant Professor, Department of Computer Applications, Islamia College of Science and Commerce, Srinagar,J&K,INDIA
4Teaching & Research Assistant, Department of Computer Application, Mewar University, Rajasthan, INDIA.

ARTICLE DETAILS

Article History
Published Online: 25 May 2019

Keywords
CCBDKT, Wireless Sensor Network, Dynamic Keying, VEBEK.

ABSTRACT

Sensors are small strategies that are used to sense the real world attributes such as temperature, humidity, flow of air and water, vibration, etc. Many applications use these sensors to predict the real world happenings and necessary actions are taken by the applications accordingly. Instead of using the sensors directly in the field, they are fabricated in the electronic devices called sensor nodes. Our proposed CCBDKT framework uses the dynamic keying technique which therefore achieves a successful packet return and data access at the receiver, for better data security against intrusion attacks.

1. Introduction

Sensors are small strategies that are used to sense the real world attributes such as temperature, humidity, flow of air and water, vibration, etc. In recent years, many applications use these sensors to predict the real world happenings and necessary actions are taken by the applications accordingly. Instead of using the sensors directly in the field, they are fabricated in the electronic devices called sensor nodes. The sensor nodes are the devices that consist of processing unit, memory, one or more types of sensors, battery and transceiver. In the homogeneous sensor networks, the lifetime of the network depletes quickly because a few or more number of nodes are doing more tasks than others. To overcome this issue, the heterogeneous sensor nodes ensure been introduced. The heterogeneity of the nodes could be classified as the link heterogeneity, computation heterogeneity and energy heterogeneity. The advantages of using the heterogeneous nodes are increased lifetime, improved reliability and less latency of data transmission. In this learning, the heterogeneous nodes with long lifecycle batteries have been included as CHs in the network that can perform aggregation, fast data transmission, clustering and a few security tasks. Also the CHs are allowed with GPS to identify its location. There are many challenges in WSN which are the conversion of raw data to digital form, robust operation, openness and heterogeneity, security, real-time and control, harsh environmental situations, reliability and latency supplies and packet mistakes. The applications of WSN in environmental checking can be generally considered as indoor and outdoor applications. Among these, the indoor applications include SMART home, SMART office, fire detection and civil arrangements deformations detections. The outdoor applications comprise Chemical dangerous detection, weather forecasting, detection of natural disasters and habitat monitoring.

2. Literature Review

Most developments in modern network security have come from cryptography in the early 1970s as a way of developing strong protocols for authentication. The National Bureau of Standards (NBS) in January 1977, which was established as the landmark for introduction cryptography examination and innovation in the modern era of computing technology, adopted the Data Encryption Standard (DES) as a data encryption average. This was another breakthrough after a new approach was suggested, which is still under progress for research (Levy, 2001), to improve public key cryptography (PKC). Cryptography helps as the basis for most IT safety solutions, including digital names for verifying the validity of changes to operating systems, staff bank, e-business and other Web-based applications that depend on heavily on SSL and TLS for verification and data protection. A layered security strategy and powerful cryptographic techniques were considered as a feasible cheap solution to secure mobile application networks by the design of the Mobile Application Security System (MASS) (Floyd, 2006). Eventually, a new concept known as Quantum Encryption, which usages quantum laser light variations on the physical surface of the current transmission cables, is regarded as a way of providing ultra-secure transport network and near-perfect protection (Hughes, 2007).

Ossama Younis and Sonia Fahmy have suggested hybrid energy effective dispersed clustering (HEED) protocol in ad hoc sensor networks that periodically selects the CHs using a mixture of their node nearness to its neighbors or node degree and residual energy. With respect to the handing out cycles and communications exchanged, the protocol attains low overhead and uniform CH distribution. Each node can operate as both source and server; thereby the servers are designated based on the goals of the system. Hence, a node has the knowledge of the servers that are located only inside its range. Global aims are attained by wise local conclusions. The simulation outcomes indicated that HEED improves the network's survival. Collections show numerous attractive HEED features. But only one layer of cluster exists here.

Dilip Kumar et al. was proposed to incorporate the energy efficiency cluster (EEHC) scheme for WSNs. In EEHC, the impact of node heterogeneity has been analyzed in terms of the energy spent. The authors assumed that the nodes are hierarchically

clustered. The CHs are elected by calculating the weight value using the early energy of a node comparative to the energy level of the neighboring nodes. In homogeneous gathering protocols, all sensor nodes with the identical energy are considered. Therefore, there is no presence of node heterogeneity. Heterogeneous nodes are used to rise the network period and reliability Due to the availability of the heterogeneous nodes inside the network, the lifetime and reliability of the WSN has been improved.

Md Enamul Haque et al. have remained suggested as a context-aware collecting hierarchy (CACH) protocol for WSNs which depends on the sensed data related to the situation (i.e. the environment background). Similar network data traffic can be avoided by CACH. CH's function can also be divided between the nodes. The output indicates substantial energy improvement. CHs are selected for energy consumption dissemination. In addition, the packet containing the same value is not sent to minimize transmission between nodes and CHs. The outcomes of the simulation demonstrate that the decreased data flow guarantees longer network idleness and durability. Nonetheless, this method will not be used for the great number of sensor nodes and the super-clustering is not deliberated here.

Mao Song et al. have suggested an energy-efficient unequal gathering procedure for big scale WSN. This algorithm balances the node power consumption, extends the network period, and attentions on energy effective unequal gathering and inter-cluster steering. Fuzzy logic arrangement is used to consider the local information of each node such as distance to BS, energy level, and limited density. Fuzzy logic scheme determines the node's probability of fetching CH and estimates the capability radius. Optimize energy responsive inter-cluster routing among CHs and BS for efficient max-min ant colony optimisation. This algorithm balances the energy use of CHs with the issue of hot spots in the WSN dynamic routing multi-hop. The results showed that this algorithm has a higher performance than other approaches such as LEACH and in energy efficiency unequal clustering (EEUC).

Marco Valero et al. have proposed distributed security framework for HWSNs (Di-Sec). Di-sec is highly independent, flexible and scalable framework that offers security against numerous attacks. In Di-sec, there is a monitoring core (M-Core) module responsible for monitoring both the insider and outsider attackers. Di-sec also provisions the detection of numerous attacks and defense against the attacks. Along with Di-Sec, the authors produced a domain exact language defined as M-core control language (MCL) which can interacts with the outline. DDMs are implemented against jamming attack, Sybil attack, selective advancing attack, and interior attacks. However, the number of M-Core services, the detection of attacks and defense coverage are less.

3. Methodology

3.1. Combined Cost Based Dynamic Keying Technique (CCBDKT)

Our Framework Proposed a scalable technique called Combined Cost Based Dynamic Keying Technique (CCBDKT) for confirmation has been suggested for heterogeneous WSN. For each sensor node, the CH specifies a Combined Cost Value (CCV), depending on the location of node, node and digital battery power. Since the key changes dynamically in the encryption system. When a change occurs in a CCV, each CH produces different dynamic keys. The source CH passes the data through various CHs sideways the Path towards the sink using RC5 encryption mechanism and is in a position to test authenticity. When the source CH wants a data packet to be transmitted to the sink, the packet is divided into portions by a secret procedure and transfers to the sink by means of a multi-path routing method. In this study, a scalable dynamic keying technique called CCBDKT for H-WSN has been proposed. The nodes are at first grouped according to distance into numerous clusters. The GPS nodes are selected as CHs. All members of the cluster can estimate their position with the aid of CH. By estimating their neighbors, every member of the cluster also estimates their node degree. The CH has a table with each member location, Id, node degree and digital energy to refer a packet to the CH. The CH will then describe a CCV on the basis of these parameters for each sensor node. This CCV is also kept in the plate. The encryption key used alters dynamically according to the CCV function. The re-keying process is not required. In each cluster the CH therefore produces separate dynamic keys. The source CHs forwards data by using the RC5 authentication mechanism through various clusters on the way to the dish, checks that the data is authentic and complete. When the distributed data packet is to be transferred to the sink, CHs divides the packet into q share as per the (t, q)–secret distribution threshold procedure. The dispersal routing multi path is used to move a quantity of shares to the sink node.

3.2. Cluster Formation

The scalability of the network can be improved by grouping the nodes into various clusters. For every cluster, there will be one CH where it performs more tasks than the normal sensor nodes. So the energy in the CH decreases rapidly associated to the normal sensor nodes. If the network contains of similar type of nodes, the lifetime of the network will be reduced. In this study, the CHs are expected to be more prevailing than the normal nodes. The nodes that are enabled with GPS will be selected as CHs.

Let S be the sink node, N be the number of sensor nodes in the WSN, each node is denoted as Ni where $i \in \mathcal{N}$, $\mathbb{C}$,be the number of CHs enabled with GPS in the WSN and each CH is denoted as CHj where $j \in \mathbb{C}$. The set of actions taken by the network to form clusters are given below:

Step 1: S sends a cluster head notification CL_NOT message to all CHj. The CL_NOT message consists of the fields such as S, CHj, CL_NOT and t (time stamp).

Step 2: Upon receiving the CL_NOT, each CHj broadcast a "HELLO" message sent to its neighbors. The "HELLO" message consists of the fields such as CHj, HELLO and t.

Step 3: Upon receiving the HELLO communications by the sensor nodes Ni, they estimate the distance Dij between the sensor node and the CH using the maximum communication power (pm), the received power (pr) from the CHj and communication range of the sensor nodes (R) as:

$$D_{ij} = \frac{\varepsilon\sqrt{p_m/p_r}}{R}$$

Step 4: The Ni sends the REPLY message to CHj which consists of the calculated Dij.

Step 5: Once the CHj receives the REPLY messages from its neighbors, it includes the neighboring sensor nodes such that Dji <Dij.

Step 6: If a node Ni does not accept any HELLO message, then it declares itself as CH and broadcast a declaration message D_MES to its neighboring nodes.

Step 7: This process is repeated by all CHj until all Ni are included in any one of the clusters. Once all the nodes are associated with the CH, they sense its intended data and

Transmit to the S through CH.

3.3. Virtual Battery Power

The Virtual Battery Power (VBP) has been considered for generating the dynamic key for every session since the real battery power consumption varies among the nodes. However, power consumption discrepancies between the nodes can lead to synchronization problems that lead to further packet falls. Every Ni sensor node is believed to have some uniqueness of VBP when first used. The sensor node goes through multiple operational stages, including node-stay-alive, packet reception, encoding, transmission and decryption. The sensor node transfers data from another sensor node or injects its own data into the network during those statements. Accordingly, the corresponding energy is the following based on the actions of the node:

Prx Reception power

Ptx Transmission power

Penc Encoding power

Pdec Decoding power

Pa Power necessary maintaining the node in the active state.

Psync Power operated to coordinate the source

PMAC Power necessary to produce MAC code

Pauth Power necessary for authentication

If any event is identified by a Ni origin node, the duration packet (ć) is forwarded to the S. This origin node is determined using the following formula to evaluate the digital value.

$$V_{cs} = \iota \times (P_{tx} + P_{enc} + P_{MAC}) + t \times P_a + P_{SYNC}$$

Where t = period of active state of the node.

When a cluster head gets information from the VBP member's node, the value of the actions taken by the recipient can be changed by decreasing. The intermediate node (Vci) digital v alue is determined using the following formula.

$$V_{cj} = \beta \times (P_{rx} + P_{auth} + P_{dec} + P_{tx+} P_{enc}) + t \times 2P_a$$

Thus, the VBP transient value is achieved by minimizing the previous VBP (Pi), which is represented using the following Equation

$$V_{BP} = \begin{cases} P_i - V_{cs}\,; if\ the\ packet\ is\ received\ from\ \text{the}\ Sender \\ P_i - V_{ci}\,; if\ the\ packet\ is\ received\ from\ \text{the}\ intermediate\ node \end{cases}$$

Where Pi = previous VBP. After all action, each node calculates and informs the transient value of VBP.

4. Dynamic Key Generation

The KD of length 128 bits is produced centered on the passing values of the CCV as KD ← f(CCV). The encoding instrument discusses to the RC5 encryption mechanism. Based on the suitable level of safety that is required for the application, the key length can be increased. The key to RC5 is generated dynamically. Other than the NL and ND, the VBP changes dynamically The sensor nodes move through a variety of operational states. The operational states include active node status, packet response and packet transmission, and encoding in addition decoding stages. During the initial network deployment, each sensor node was initialized with VBP. In the functional states described above, the VBP is reduced accordingly. The unpredictable change in the VBP is used for dynamic key generation which is explained below. Let VBPc be the current value of the VBP, Fk be the key generation function, Ci be first cost of the sensor node, Ck be the present cost value reorganized by Rc, KD(i) be the Current KD, KD(i+1) be the Next KD, and Vi be the initialization vector. The VBPc of the node used as the key to the permutation function Fk. When the sensors are originally deployed, they comprise Ci and hence the first dynamic key KD(i) is generated as the function of the Ci and Vi i.e. KD(i) = Fk (Ci, Vi). The Vi value is distributed to the sensors and it is used to generate the first key and the it is discarded. Consequently the next dynamic key KD(i+1) is generated as the function of KD(i) and Ck i.e KD(i+1) = Fk (KD(i), Ck). The function Fk generates the key using t- degree polynomial. Every received packet is connected to a new distinctive key which is produced founded on the transient values of the VBP and this aspect is assured by the virtual battery power keying module. When the data is detected and

therefore no different procedure is necessary to modify the keys, the key generation scheme will be initiated. The dynamic key calculation algorithm is:

1. Initialize, i = 1
2. Begin
3. If i = 1
4. Then
5. KD(i) ← Fk (Ci, Vi), i ← i+1
6. Else
7. KD(i+1) ← Fk (KD(i), Cc), i ← i+1
8. End if
9. End

The CH getting a packet from a node also generates the KD using the same algorithm for decryption and verifying authentication. The packet comprises the fields such as destination ID of CH, type and data arenas composed signified as z. This packet is forwarded to the CH of each SN. According to the RC5 method, z is pseudo randomly transmitted. The packet that is to be transmitted contains the message Z encoded by key KD[ID{KD(z)}] and the message KD (z). When a packet is received by the next CH along the sinking path, it produces a KD to decode the packet locally.

The origin node must hold protected reports after the event detection and uses the VBP to construct the next button. The key is offered to produce a permutation code for encoding the z message in the encoding module as an input to the RC5 algorithm.

5. Multi-Path Dispersal Routing

5.1. Dispersal Technique

The packet divides the packet into q pieces by (t / q)–the hidden algorithm limit, if the CH has to direct the aggregated information packet to the sink. For examples. The algorithm of Shamir. The object of this scheme is to cooperate with groups of mutually suspects with conflicting interests. This module's useful properties are

- The shares ' volume does not surpass the original data value.
- If the t is retained, shares can be further or removed dynamically without impacting the other shares.

The dispersal route for multipath is used to forward the portions to the following CH. Each part contains a TTL ground that is awarded to control the total random transmission amount by the source node. After each transmission, the value of the TTL field is increasing by 1. The last CH to receive the shares starts transmitting the TTL field to the sink after it reaches zero. If the sink receives at least t bytes, the original packet can be reused.

5.2. Multi-path Routing

For transmission of q sharing after CH to the sink, multi path routing is created. The multi-way routing protocol typically prefers the node disconnected paths because the network's most available resources are used. The following stages were carried out to carry out the path discovery:

Phase 1 - Initialization Phase: All CH sends a “HELLO” message across the network to provide sufficient information about its closest neighbors. The “HELLO” message contains evidence including origin description, hop count and VBP. In this step, CH manages and uploads a buffer table that contains the neighboring CHs list data, the VBP Free buffer origin ID Hop count.

Phase 2 - Route Discovery Phase: Since step 1, the information for the measurement of the costs of the neighboring CHs is stored in each CH. The next-hop CH is determined from the source CH (CH4). It then transmits the message RREQ to the next hop CH selected. The RREQ message contains the source ID, endpoint ID and cluster ID. The next CH hop from the source CH also determines its chosen next hop of the sink node path and carry on until the RREQ message hits the sink node. To avoid getting paths with mutual CHs, each CH node accepts only one RREQ message. If a CH receives two or more RREQ messages, only rejecting other messages is accepted.

Once all the RREQ messages have been received, the sink note answers CH4 back using the RREP message via the RREQ messages. CH4 will classify the available roads and will share these roads in the direction of the sink node on the basis of the RREP.

6. Experimental Setup

The implementation of the planned dynamic keying technique CCBDKT is done in C++ and verified in NS2 with 2.32 TCL simulation scripts. The performance of CCBDKT and VEBEK are tested in a number of simulated scenarios. The simulation scenarios have been created by changing the amount of nodes and the number of attackers inside the network

6.1. Simulation Parameters

For the purpose of determining the values of normalizing constants α, β and μ the simulation configurations for the performance measurement of CCBDKT and VEBEK are given, we consider their values between 0 and 1 to be α + β + μ 1 At the beginning, α is taken as 0.2 or β and μ is assumed to be 0.2.

No. of Nodes (n) hundred to five hundred

Area Size is 500 m × 500 m

Simulation Time is 300 secs
Routing protocol Multipath Dispersal Routing
Radio Propagation Model and Two-Ray Ground model MAC IEEE 802.11
Antenna Type Omni Antenna
Traffic Source CBR
Transmission range CH: 100 m SN: 50 m
Reception power 0.0648W
Transmission power 0.0744W
Idle power 0.00000552W
Initial Energy 18 Joules
Initial VBP 250 Joules
No. of attackers 5 to 25

6.2. Performance Metrics

The performance of CCBDKT is associated with the VEBEK schemes created on the subsequent metrics:

Energy Consumption: It is the normal energy spent for the data transmission. The network lifetime is indirectly or inversely proportional to the power consumption. If the power consumption of the whole network is high, the network lifetime will be low.

Data Availability: It is the percentage of data that are positively transported at the destination in the presence of attackers.

Average Packet Delivery Ratio: It is the proportion of the amount of packets gained effectively to the entire amount of packets transferred.

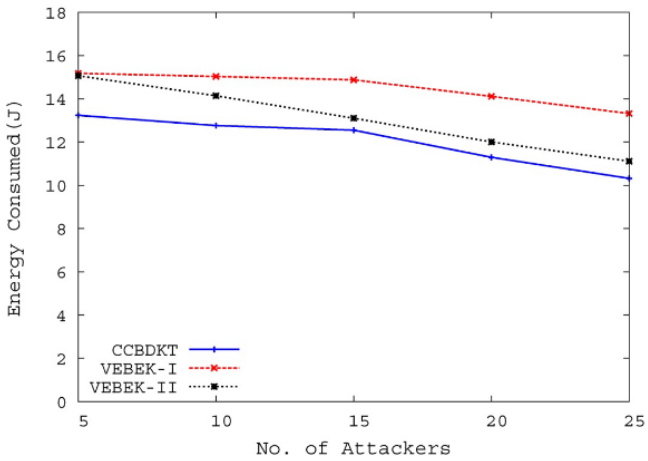
Computation Cost: It is the cost calculated in terms of energy spent for generating dynamic keys.

7. Results and Discussions

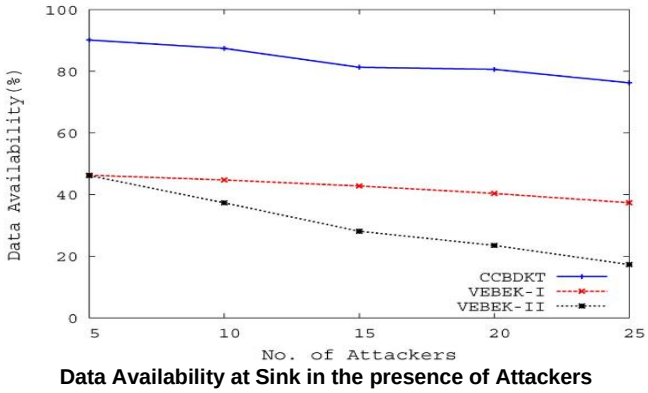
This segment presents the simulation and performance consequences of the proposed CCBDKT associated with the present technique VEBEK. The results are shown one by one along with the discussions.

7.1. Results by varying the number of attackers

The amount of attackers from different clusters executing black hole and packet drop offs ranges between 5 and 25 in the initial simulation. The network's amount of nodes is set to 100.The figure demonstrations the average network energy consumption, including calculation and communication tasks. energy consumption From the figure it is revealed that, if the amount of attackers is increasing, the average power consumption falls. Because of the drop in packets and black hole attacks, more packets are dropped. So the energy consumption decreases if the attackers are increased.

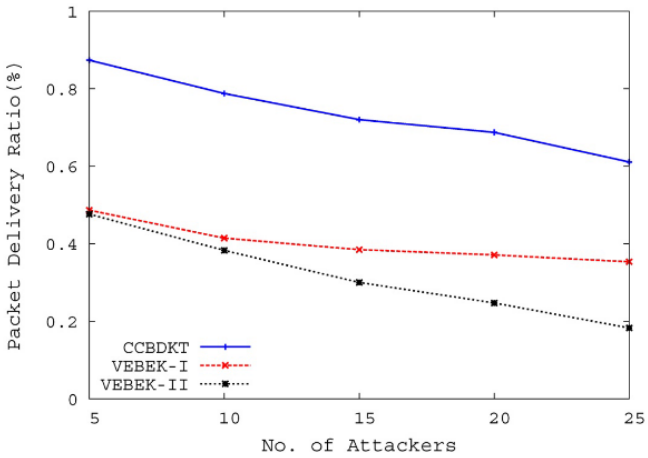


Average Energy Consumed in the presence of Attackers

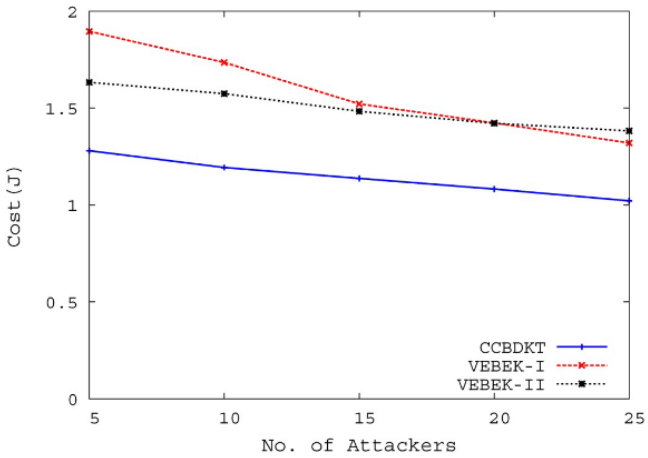


Data Availability at Sink in the presence of Attackers

Every node in VEBEK-I watches all its neighbours transaction. But in VEBEK-II only watches some selective nodes only. Hence VEBEK-I consumes more energy than VEBEK-II. When the forwarding node in VEBEK can not successfully extract the password, it tries to mark the packet as malicious by another key. Since the simulation begins an attack on the packet drop along the sink path, transmission nodes proceed to retrieve the key even if the packet is not malicious. It therefore consumes further energy than CCBDKT. Figure shows the percentage of data that are successfully retrieved by the sink. The data from the source CH are transmitted to the sink by segmenting the data into various packets. If all the packets that belong to a payload are delivered at the Sink, it can be able to save the entire data successfully. If not, the entire data cannot be retrieved using a few numbers of packets established by the sink. Since CCBDKT uses multi-path dispersal routing method, the sink reconstructs the data by receiving at least t out of n shares. Thus the CCBDKT achieves higher percentage of data availability at the Sink compared to VEBEK-I and VEBEK-II. The VEBEK-I filters all the false packets in the next hop itself. So the false packets are not forwarded in more numbers inside the network and thus the traffic is not increased. But in VEBEK-II, it filters the false packets but not in the immediate next hop. Hence a few numbers of false packets are travelling inside the network. This increases the network traffic and so more number of legitimate packets is released inside the network. Since the legitimate packets are released by the attackers as well as due to the increase in traffic, the data can not be retrieved completely at the Sink.



Average Packet Delivery Ratio in the presence of Attackers



Computation Cost in the presence of Attackers

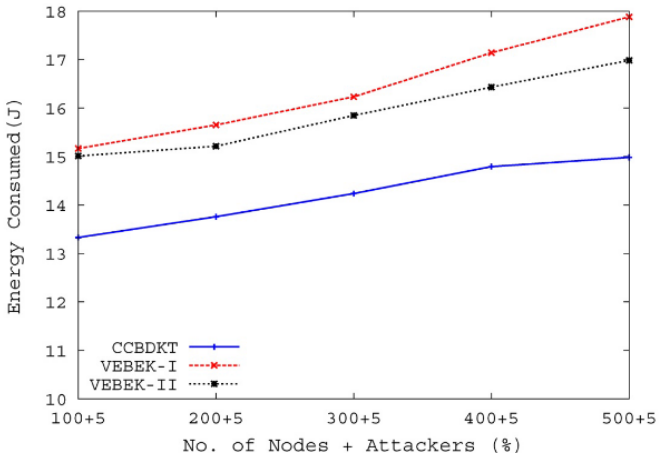
Figure demonstrates the regular packet delivery proportion in the occurrence of the attackers. The attackers are varied from 5 to 25. Since the attackers drop more number of packets, the packet delivery proportion is decreasing. Due to the multi-path dispersion method, CCBDKT provides good PDR associated to VEBEK-I and VEBEK-II, because the packets from the source CH travels through multiple paths to the destination. VEBEK-I provides better PDR than VEBEK-II because the false packets are discarded in the next hop itself. If the attacker exists in a path to the destination, mostly all the packets are dropped by the attackers because VEBEK does not use multi-path routing.

Figure shows the computation cost in terms of energy consumed for performing the computations other than transmission and reception. The VEBEK-I and VEBEK-II tries to classify the false packets by using as many keys as possible until it reaches virtual Key Search threshold level. So the computation cost will be high. In CCBDKT, the false packets are discarded at the CH level by verifying the authenticity of the packets sent by the attackers.

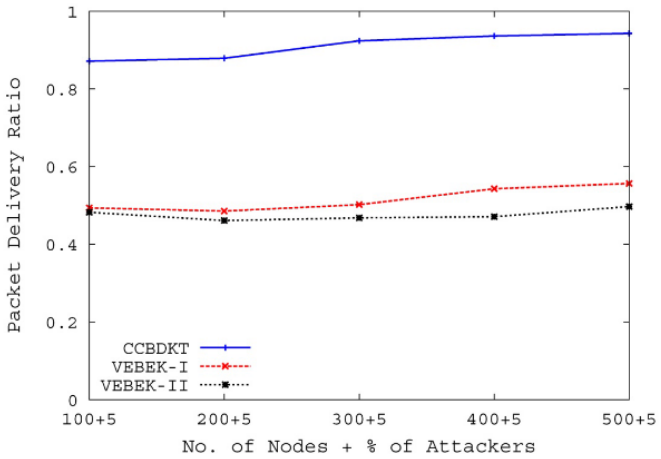
7.2. Results by varying the number of Nodes

Followed by the simulation of changing the numbers of attackers, the results have also been obtained by changing the network size from 100 to 500. In this simulation scenario, the numbers of attackers are fixed as 5 % of the node size.

Figure displays the average energy consumed by the network while increasing the amount of nodes in the network. The quantity of attackers is 5% of the total amount of nodes in the network. Due to the rise in number of hops and the verification of authentication and integrity, both VEBEK-I and VEBEK-II consume more energy than CCBDKT. Also every node in VEBEK-I watches all its neighbors transaction, it consumes more energy than VEBEK-II. In VEBEK-II, only a few identified nodes in the watching list are watched. Also the VEBEK-I and VEBEK-II tries to classify the false packets by using as many keys as possible until it reaches virtual Key Search threshold level.



Average Energy consumed by increasing Network Size



Average Packet Delivery Ratio by increasing Network Size

Figure displays the packet delivery proportion by growing the amount of nodes in the network. The quantity of attackers is 5% of the total quantity of nodes in the network. In CCBDKT, if the network size increases, there exist a more number of paths to the Sink. So the multi-path spreading method performs well to deliver the data at the Sink. In VEBEK-II, there is no development in the packet delivery ratio. But the VEBEK – I performs better due to the hop by hop authentication and integrity verification. Since VEBEK uses directed diffusion, more numbers of legal packets are dropped in the presence of the attackers. So the packet delivery ratio is very less associated to CCBDKT.

8. Conclusion

In this paper, the generated dynamic key is used for authenticating the packets arriving at the CHs. Initially the network is separated into collections called clusters. The normal sensor node identifies its nearer heterogeneous sensor node and associates with it. Once the clusters are made, the sensor nodes generate the dynamic key using a dynamic value called CCV.

The CCV is calculated using the parameters NL, ND and VBP. Since the network in this study is static, the NL and ND do not change. But the VBP changes for every data transmission and reception. Due to the changes in VBP, the CCV value also changes frequently which cannot be predicted by the intruders. Using the CCV value, the dynamic key is generated and used for encrypting the data as well as for generating MAC value for authentication. The CH upon receiving the packets authenticates the packets by generating the same dynamic key used by the sender. Due to the authentication, the false packets are identified and discarded at the CH level itself. Using the threshold covert algorithm, the CH adds and transfers the data to the Sink by splitting data into different shares and forwarding them with a multi-way dispersal routing technique. Upon getting the data from sensor nodes. The CCBDKT therefore achieves a successful packet return and data access at the receiver. In relations of available data, the packet delivery proportion, average power consumption and computation costs, the presentation of CCBDKT was tested and associated with VEBEK-I and VEBEK-II. The findings of the simulation show that the CCBDKT is well working relative to VEBEK-I and VEBEK-II systems.

References

[1] Haijun, L and Chao, W, An Energy Efficient Dynamic Key Management Based Polynomial and cluster in wireless sensor networks. Journal ofConvergence Information Technolog, 6 (5) (May 2011), 321-328.

[2] Haque, Md.Enamul, Matsumoto, Noriko, and Yoshida, Norihiko, Context aware cluster-based hierarchical protocol for Wireless Sensor Networks. International Journal of Ad Hoc and Ubiquitous Computing, 4 (6) (2009), 379-386.

[3] Rivest, R.L., Shamir, A., and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. In Communications of the ACM(New York, USA 1978), ACM, 120-126.

[4] Jiang, Yixin, Lin, Chuang, Shi, Minghui, and Shen, Xuemin (Sherman), Self-healing group key distribution with time-limited node revocation for wireless sensor networks. Ad Hoc Networks, 5 (1) (2007), 14-23.

[5] Kumar, Kamal, Verma, A.K., and Patel, R.B., Framework for Key Management Scheme in Heterogeneous Wireless Sensor Networks. Journal of Emerging Technologies in Web Intelligence, 3 (4) (November 2011), 286-296.

[6] Kumar, Pardeep, Ylianttila, Mika, Gurtov, Andrei, Lee, Sang-Gon, and Lee, Hoon-Jae, An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor network-based applications. Sensors(Base), 14 (2) (February 11, 2014), 2732-55.

[7] Martin, Keith M, Paterson, Maura B, and Stinson, Douglas R, Key Pre-distribution for Homogeneous Wireless Sensor Networks with Group Deployment of Nodes. ACM Transactions on Sensor Networks (TOSN), 7 (2) (2008), 1-18.

[8] Mishra, Sushruta, Thakkar, Hiren, Chakrabarty, Alok, and Kimtani, Deepesh, Dynamic Cluster Based Data Aggregation in WSN (FDDA). International Journal of Electronics Communication and Computer Technology (IJECCT), 2 (5) (September 2012), 227-230.

[9] Raymond, David R. and Midkiff, Scott F., Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. Pervasive Computing, 7 (1) (2008), 74-81.

[10] Ssu, Kuo-Feng, Wang, Wei-Tong, and Chang, Wen-Chung, Detecting Sybil attacks in Wireless Sensor Networks using neighboring information. Computer Networks, 53 (18) (2009), 3042-3056.

