JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1523 - 1532
https://publishoa.com
ISSN: 1309-3452

High-Level Security Approach in Wireless Sensor Network using Cluster Based Dynamic Keying Technique

[1]Dr. Khair Ul Nisa
Assistant Professor (C), Dept. of Information Technology,
Cluster University Srinagar, J&K, India,
(S.P.College, Srinagar)
Email: dr.khairulnisa.it@gmail.com

[2]Dr. Mujtaba Ashraf Qureshi
Assistant Professor (C), Dept. of Information Technology,
Cluster University Srinagar, J&K, India,
(AAAM College, Srinagar)
Email: mujtaba170@gmail.com

[3]Aijaz Ahmad
Assistant Professor, Dept. of Information Technology,
Cluster University Srinagar, J&K, India,
(S.P.College, Srinagar)
Email: khaki.aijaz856@gmail.com

ABSTRACT

The security of a network relates to all the functionality, operating procedures and steps required to ensure an appropriate level of security and confidence for network-wide data transmission, access control and administrative policies and management policies to ensure the honesty, accessibility and privacy of data at the same time. In this method, cryptographic strategy CBSDKT is used to detect any infiltration attack during data transmission between wireless sensor networks (WSNs). Also, this research work presents the simulation results at/using different parameters which depicts/presents exceptional results which help to maintain Wireless Network Sensor transmission of data secure.

Keywords: WSN, Network Security, CBSDKT, Cluster Head.

1. Introduction

As information technology is becoming increasingly prevalent in almost every aspect of our lives, particularly with the advent of e-commerce platforms and social networks, the amount of data produced and stored continues to grow at an astounding rate which requires improved data security mechanisms to ensure the safe transmission of data through networks. Network security continues to be an interesting field primarily because of increasing number of intrusions taking place every day. Apart from human origin (called intruders), security can be breached by natural disasters, catastrophic failures and many other sources. Wireless sensor networks (WSNs) are more extensive and prevalent in assorted spheres (army, health, etc). So, these networks need extraordinary level of

security **[1].** Threats, except from those that originate from people are not a major cause of concern. These however, can be dealt by keeping copies of data at different locations, keeping backup generators and so on. The intruders find one way or the other to breach into the computing system to compromise the security model of an organization. Information security in substructure less wireless sensor networks (WSNs) is one of the utmost significant research trials. In such networks, sensor nodes are usually scattered profusely in the field in order to display, fold, broadcast, and deliver the recognized data to the expertise node **[2].** This puts a challenge in front of security engineers who continuously work to identify the loopholes and limitations of these security measures and try to improvise accordingly. The fact, a computing system is not only insecure from the external environment; identifying the intruders from within the system is in itself a difficult if not impossible task. The use of secure tunnels as a solution to improve the protection of WSNs can be employed **[4].**

Dynamic Key Management for Mobile WSNs:

The mobility of sensor nodes is important in different medium and large-size real time systems in Heterogeneous Wireless Sensors Networks, such as event identification, location, medical monitoring, transport and multimedia. A secure wireless sensor network (SWSN) communiqué protocol depends on an effectual key controlling and management coordination **[3].** The mobility of nodes leads to random, regular topological changes. The clustering must be carried out dynamically due to the topological shifts. For clustering in a mobile WSN, Hong suggested a weight based clustering algorithm.

Current clustering algorithms including hybrid, energy-efficient, dispersed clustering (HEED) are an extension of the simple LEACH protocol which utilizes residual power and clustering node size, energy-efficient heterogeneous clustering schemes (EEHCs). The CH is selected centred on the mass value that is determined by strictures such as the node grade difference, amount of distances after a node to its neighbours, rate of movement, sensor node feature, amount of times a node is CH. The node is selected as CH with a minimum weight value. The safety is compromised in the mobile network environments since the nodes in the network often switch. When developing a strategy, the security standards are met:

Freshness of key: Due to the node mobility, the key(s) essential to be efficient and made existing between completely the SNs and the CH. A secure wireless sensor network (SWSN) communiqué protocol depends on an effectual key controlling coordination **[3].** A key management protocol for assorted sensor networks based on an unbalanced cryptosystem named pairing identity created cryptography was employed **[6].**

Authentication of nodes: To or from any CH, any node may join. Each heterogeneous node may likewise become such a cluster CH. The nodes must be authenticated because of these dynamic changes.

Preserving data integrity: Due to changes in topology, the data should be modified by no adversary.

A complex key management approach for group-based sensor networks, oriented on EBS (Exclusion-Based Systems), is the Localized combinatory key (LOCK). LOCK involves re-keying if the node capture probability exceeds a certain threshold. Ozgur suggested the multi-level hierarchical key management scheme using UAV, an asymmetric key distribution and coordination Centre. This device constructs symmetrical keys for further interaction using asymmetric keys. This structure depends heavily on UAV, which is physically susceptible. A static dynamic key management protocol that uses the separate safety requirement of WSN has been suggested by Tim Landstra et al. Generally there most of the intrusion detection system operate at one layer of OSI model, however a new intrusion detection system based on cross layer interaction between the network, Mac and physical layers have been proposed **[5].**

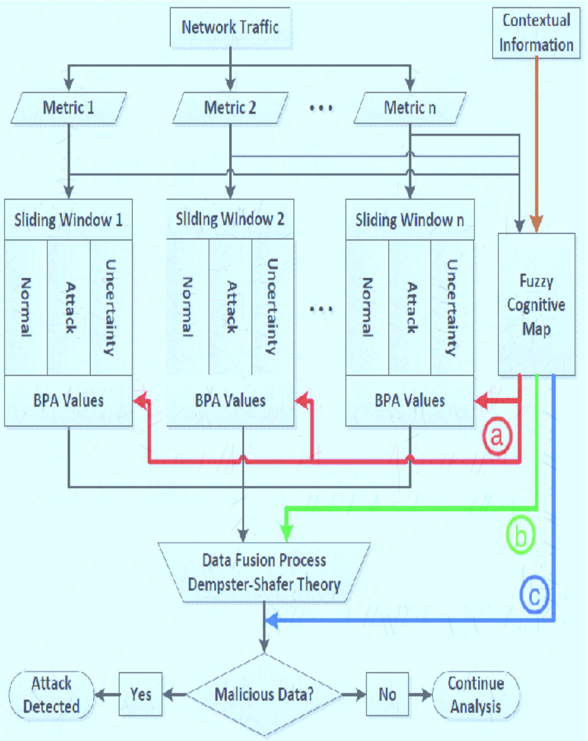

Figure 1: Schematic Structure of IDS.

This protocol is used to create sub network around an event with a self-organizing protocol. Most networks run in low-security mode in this configuration with still power saving keys. The rest of the network or sub-network works with dynamic keys in high-security mode.

2. Literature Survey

Jen-Yan-Huang et al (2011): In this work author proposes new key management method that practices dynamic key management arrangements for assorted sensor networks. The planned arrangement masses a hash function into the base station (BS), cluster heads (CH), and sensor nodes (SN). The cluster heads and sensor nodes then produce their individual key chains to deliver advancing verification in case of key changes, safety openings, and key variations because of security openings. The cluster heads and sensor nodes create in pairs the keys to guarantee broadcast privacy. The planned arrangement declines the quantity of keys prerequisite for sensor nodes and cluster heads and is strong to the subsequent bouts: predicting attacks, repeat attacks, man-in-the-middle spasms, node seizure spasms, and denial-of-service spasms.

P. Kumar et al. suggested a joint verification and dynamic model that is ideal for heterogeneous real-time WSNs. During the cluster creation and new node addition, mutual authentication takes place under this scheme. The dynamic session keys are produced via the dynamic secret sum dynamically produced from H-sensors and for encryption the dynamic session key is used.

Qiu et al. introduced a broad, flexible and distributed WSN authentication scheme. The problem in the works currently underway is increased processing overhead, overhead connectivity, the relevant security solutions for static networks only, dependence on a central authority or instrument, provided that static or preloaded keys, etc. The result offered seeks to resolve the issues described overhead. The strategy suggested for mobile WSN applications in this study can be extended because it takes the node position into the complex key generation system into consideration. It also reduces overhead interaction. The key distribution and coordination system does not rely on a single device, because only the CHs and sinks take part in a key production process.

Yihong Zang et al. have planned secured sector grounded bi-path clustering as well as routing protocol, in which a bi-path routing algorithm minimizes the computational above and energy dissipation. A major pre-deal scheme has been proposed for sharing keys with the sensor nodes present on the road, while nodes not present on the way do not have keys with way nodes. The imitation findings display that this protocol ensures safety extends the network life and achieves high connectivity probabilities when network size is too large. Nevertheless, when a certain quantity of nodes dies and lives when the network is increasing, network survival time improves.

Jen-Yan Huang et al. have suggested a key management system in heterogeneous WSN that is made up of less number of high end sensors (Hsensors or cluster heads) and more amount of low end sensors (L-sensors or cluster members). H-sensors have increased transmission range, memory, battery power, and responsibility tolerance, whereas L-sensors are common sensor nodes with ordinary resources. L-sensors stock a little data at a time and need low memory space to operate quickly. On the basis of the cluster status, H-sensors commonly replace the encrypting key and L-sensors can regulate whether the new key is authorized or not. This strategy necessitates only some possessions to attain the security, while ensuring integrity, confidentiality, and availability. The power consumption of this scheme can be calculated in terms of the amount of existence nodes over several circles. During simulation in each round, H-sensor needs and collects the statistics from all L-sensors and from a exact L-sensor.

Seung-Hyun Seo et al. have planned a certificate-less active key management (CL-EKM) system for dynamic WSNs. CL-EKM recognizes four key types that are every used for a variety of purposes, comprising stable, pair-sided node communication and group-oriented cluster key message. Well-organized key management processes are clear as promoting node movements' crossways the dissimilar clusters. The test results demonstration that the CL-EKM model is lightweight and therefore appropriate for complex WSNs. Nevertheless, the consumption of energy is more important than the life of the network

3. Methodology

Cluster Based Secure Dynamic Keying Technique:

The present study proposes a Cluster-based Safe Dynamic Keying Method (CSDKT), which provisions malicious and mobility node detection techniques, for an H-WSN authentication. In this procedure the high-power heterogeneous nodes are selected as CHs once nodes are arranged in the field. GPS makes the CHs. The nodes are selected as CHs with minimum weight values. The weight value of the ND, Dav, Sav and VBP is calculated. Once the CHs are chosen a value called CCV

must be determined by each node in the network. The CCV is the dynamic key to be used by nodes to protect the data in future communications. Regularly updated by changes in the CCV value, dynamic keys determined by the nodes. The re-election of the CH occurs by the cluster members while the CH tends to leave the network. The flexibility of the cluster members and CHs is authenticated using the dynamic key to ensure network security. The malicious cluster leaders and CHs from the network are excluded using a bidirectional identification technique for malicious nodes.
Boulis (2011) Castalia, a simulator for Wireless Sensor Networks (WSN), Body Area Networks and usually networks of low-power fixed devices. This is grounded on the OMNeT++ stage and can be castoff by academics and designers who need to trial their dispersed algorithms/protocols in accurate wireless station and broadcasting models, with a accurate node performance particularly connecting to admittance of the radio **[7].**

Network Model:
An H-WSN supporting the node mobility within the network was identified in this analysis. The network comprises BS (also called sink), CH and resource limited SNs. These include a greater power, storage and processing ability in terms of the BS and CHs compared with SNs. The CH numbers vary depending on the grid size. The SNs collect and send the readings to the CH depending on the request. If a CH must send its data to the dish, then it differences the packet into different shares by a hidden threshold sharing procedure and transfers it to the dish via several paths. The Multipath Dispersal Routing is called this Routing Method. BS, CH and SNs are fixed within the network in this network. The applications ' clients connect with the BS network. The BS gathers data sent by CHs, carries out analysis, sends commands to SNs via CH and detects malicious nodes between CHs when necessary.

Cluster Formation and CH Selection:
As the network has large nodes, these nodes are generally identified when CH. These nodes are not included. If high configuration CH is corrupted or dead, the nodes connected with that CH are disconnected from the network during much of the life time of the network. The Member nodes attempt to link with a specific CH in order to avoid this. If no other high formation CH is existing in the area, one of the normal extraordinary VBP and low Sav nodes is responsible for extending the network life as CH. The CHs are therefore chosen grounded on the value of weight. The weight values are not fixed but are measured dynamically. On the basis of parameters such as ND, Dav, Sav and VBP the nodes in the network are determined to be in weights. The subsequent steps are taken for cluster creation and maintenance: Let S is the sink nodes. Two sensors in the WSN are included; each normal node is referred to as Ni; the high formation nodes that are activated with GPS are referred to as CHi, where ltd. The following steps are taken.

Step 1: A HELLO email is sent to their neighbors throughout the Network. The nodes enabled with GPS include only their HELLO message position data. As its position, the other usual node is (0, 0). The node that collects the location data from the GPS-enabled node calculates its individual NL founded on the DRL system. The CH is known as the DRL seed node. Every time Ni travels to another situation using the CH in the goal location this NL is changed.

Step 2: All the nodes comprising the GPS permitted nodes analyze their Sav using the Equation (1.1) which is given below:

$$S_{av} = \frac{\sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2}}{\Delta t} \qquad \text{…….........} (1.1)$$

where (xt, yt) is the node coordinates Ni at time t, (xt-1, yt-1) is the coordinates of node Ni at time t-1, and Δt is the time interval between t and t-1.

Step 3: All the nodes that receive the HELLO messages calculate the Dav value using the equation (1.2) which is given below:

$$D_{av} = \frac{\left(\Sigma \frac{\sqrt[\varepsilon]{P_m/P_r}}{R}\right)}{No.of\ HELLO\ messages\ received} \qquad \text{....…….. } (1.2)$$

Where Pm and Pr are the transmission and reception powers, separately, R is the communication variety and the path loss exponent is ε.

Step 4: Founded on the established "HELLO" messages, completely the Ni calculates the node degree [117] NDi by the number of HELLO messages established from diverse one hop neighbors as follows:

$$ND_i = COUNT(N_i|D(N_i, N_j) < R_{tx}(i),\ i\ and\ j\epsilon\ \mathcal{N}) \quad \text{..……. (1.3)}$$

where D(Ni, Nj) denotes the distance between Ni and Nj, Rtx means the transmission range of Ni.

Step 5: After each node of the network calculates the CH Nomination message (CH Name) which comprises of ND, Dav, Sav, VBP and Wi, as 0, they are broadcast to all the values essential for CH election.

Step 6: Upon getting the CH_NOM messages, all the nodes analyze the Wias follows:

$$W_i = \frac{(c_1 D_{av})\times(c_2(S_{av}+1))}{(c_3 ND)\times(c_4 V_{BP})} \quad \text{………. (1.4)}$$

Where i = 1, 2, 3,... nodes, c1,c2,c3 and c4 are the weighted coefficients. The values of weighted coefficients are allocated in such a technique that c1 + c2 + c3 + c4= 1. We have assigned the values for c1, c2, c3 and c4 as 0.15, 0.35, 0.15 and 0.35 respectively. The node that is enabled with GPS is optionally chosen as CH in the normal case. In some instances, the node of reduced mobility and higher VBP must ideally be chosen as CH if no node that is allowed with GSP is available in an area. The latter arises if the CH has been affected or harmed physically. The numerator values should ideally be fewer, and the denominator values must be large, based on the formula (1.4), becoming a CH node.

Step 7: The Ni with minimum Wi is selected as the CH after the weights of the individual Ni are calculated before clustering is defined. Therefore, all NI transmits the Wi determined using the Node Weight message (NOD WGT), including data such as Wi and ts, in its transmission array. The node of minimum Wi assumes the CH in that region on the basis of such information and provides CH Information Message (CH INFO), consisting of information such as CHi ID, ND and ts to their member nodes. Taking into account a set of five nodes in an area with the test values below. The weight of the node number ten is lower among the five nodes. Thus node number 10 in that area is selected as CH. All other regions are working in the same way and the CHs are chosen.

Node Id	ND	Dav	Sav	VBP	Wi
11	5	2.6	2	33.2	0.107
12	3	3.733333	3	32.22	0.317
13	3	3.7	3	33.1	0.306
8	3	3.6	3	32.02	0.307
10	5	3.7	0	388.57	0.008

Step 8: The Ni transmits a Cluster Joints (CL JOIN) Message to the closest CHi founded on the established CH INFO communication and signal intensity. If there is a Ni node in an overlapping region, further than one CH INFO message may be received. If this is the case, the Ni chooses a CHi with good signal power as its CH and refers a message with CL JOIN. Steps 1 to 8 must be replicated if a CHi is transferred elsewhere. When a member node changes to another location, CHi members are modified and informed of the ND value itself.

Dynamic Key Generation and Encoding

The KD is produced on the basis of the transitional values of the CCV as KD for f(CCV). When a Ni node has records to be transmitted, it produces the KD by its present VBP. The Ni encrypts the information using the KD and transmits it to its corresponding CH. The same KD delivered by Ni for decrypting data must be produced if the CH receives the database. The CH produces the right KD, based on the extent of the obtained data and the previous VBP of the Ni node. The encoding scheme refers to the method of encoding of RC5. The RC5 key is dynamically produced. The packages include the ID, form and data fields, which are commonly referred to as z. This packet is sent to its CH by each SN.

According to the findings of the RC5, z is pseudo randomly conveyed. The communication z is encoded by key k in the packet to be advanced,[ID{ k (z)}] and k (z) When the following CH along the sink path gets the packet, the KD will be locally generated to decode the packet. The source node must keep secured reports after detection and uses the VBP to build the following key. The following key is used. The key to produce a permutation code for the z message is also provided as an input for the RC5 algorithm in the encoding module.

Key Updating Process

For three instances, Ni leaves a cluster, Ni enters a cluster and CH leaves the cluster, the main inform is carried out. The measures involved are shown in the corresponding algorithm in these three examples.

```
If Ni leaves a cluster then
    Ni alerts CH
    CH approves Ni
    CH recomputed CCV of its members
Else if Ni joins a cluster then
    Ni gives connection appeal to CH
    CH gives acknowledgment to Ni
    Ni notifies CH of its VBP, NL and ND
    CH confirms Ni
Else if CH verdures a cluster then
    CH informs its cluster members
    Re-election of CH taking
    New CH recomputed CCV of its cluster followers
End if
```

Malicious Node and CH Detection

The subsequent two algorithms demonstrate the malicious node detection instrument:

Malicious node Detection:

Step 1: At first each CH defines CH (TTCH) with appreciation for its sensing field, a threshold trust quality.
Step 2: CH tracks and decides if CMi is or will not be malicious by using the following two cases of trust quality of information transmitted by its cluster Member (CMi): case 1: if TCHj(t) < TTCH, then CMi is marked as malicious (MLi)
if the CMi is calculated as trusted node, the TCHj(t) > TTCH.
The Member node is calculated to be malicious if the trust value of the data collected by the Cluster member is below this threshold. It is then calculated as a node of confidence.
Step 3: Subsequent this malicious node detection, the CH transmissions the malicious node REVocation MESsage (REVMES) to its members. The communication comprises the particularity of MLi and the KD deposited in it.
Step 4: CMi on getting REVMES detaches its link with MLi and achieves key refreshment related with that node.
The malicious nodes and keys they know are removed from the network by means of this step. While the malicious cluster nodes are removed from the cluster, the CH can become a malicious node. The next step is for validating network CHs. The next step is

Malicious CH Detection:

Step 1: BS calculates TBSj (t) of CH and is confirmed with Threshold Trust Value set by BS (TTBS) using the subsequent cases:
Case 1: if TBSj (t) >TTBS, then CH will be measured as trusted node.
Case 2: if TBSj (t) < TTBS, then CH is noticeable as malicious node.
Step 2: BS broadcasts CH Invalidation Command (CHIC) to all members of the cluster following the identification of malignant CH. The BS-command of invalidation is recognized by the CMi only and exposed by the CHj, as the BS and CMi are secured by symmetrical dynamic button.
Step 3: CMi terminates the transmission of data to the malicious CH and conducts the re-election of CH when CHIC is received.

4. Experimental Setup

The proposed CBSDKT technology is assessed with the 2.32 NS2 simulator versions. The simulation takes place over 20 tests goes with different scenarios and the average for each value is given. The result is demonstrated as a 95% confidence interval error diagram.

Simulation Parameters:

The simulation parameters are shown below in lucid manner;

No. of Nodes (n) 100 to 500
Simulation Time (sec) 300
Area Size is 500 × 500 m
Traffic Source CBR
Radio Propagation Model and Two-Ray Ground model MAC IEEE 802.11
Antenna Type Omni Anenna
Mobility Model Random Way Point
Mobility speed is (m/s) 0 to 25
Pause time (sec) CH= 30, SN=10
Initial Energy(J) CH =50, SN =5
Reception power 0.0648W
Transmission power 0.0744W
Idle power 0.00000552W
Initial VBP (J) CH =500, SN =50
Radio range (m) SN = 50, CH =150
No. of internal Attackers 90 percent of attackers
No. of external Attackers 10 percent of attackers
No. of CHs 6 percent of n

5. Result and Analysis

The amount of attackers varies from 5 to 10, 15 to 20 and 25, with the number of nodes at 200. The first is calculating the median PDR.

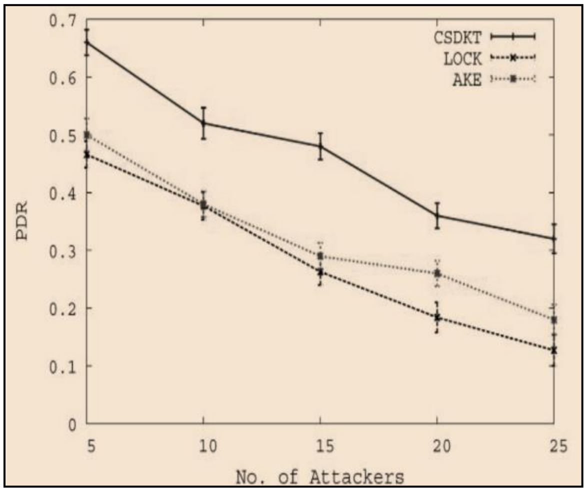

Figure 2: Packet Delivery Ratio in the presence of Attackers.

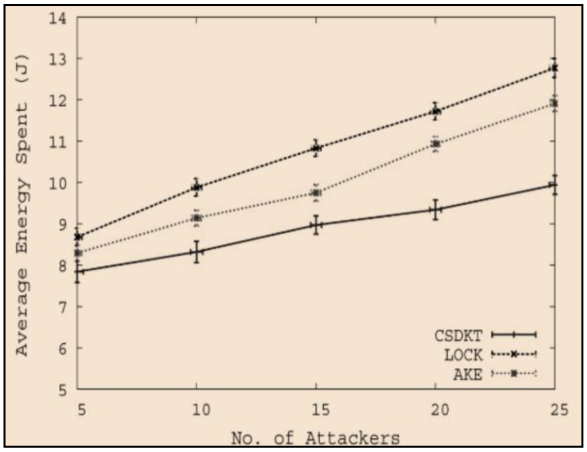

Figure 3: Average Energy Consumption in the presence of Attackers.

In this graph you can see the PDR of CSDKT, AKE, and LOCK schemes. Through means of two-way malicious node command, CBSDKT avoids malicious cluster members and CH. The number of incorrect packets in the network is limited, which means there are more legitimate packets entering their destination because Malicious Nodes are removed from the network. CBSDKT also uses a multi-path dispersal routing system that mitigates selective transmission attacks. Thus, compared with LOCK and AKE, CBSDKT performed better in PDR. Secondly, the mean energy absorbed by all nodes is calculated for data transmission. It includes energy expenditure for data transmission, receipt and calculation.

The figure-3 represents the CBSDKT, AKE and LOCK systems average energy consumption. When the amount of attackers is enlarged, the average energy consumption increases. This is because of the increase in the number of falsified network attackers. On the CH point, the CBSDKT filters bad packets. As packets are not distributed over the network, the power consumption of the attackers is lower. When capturing the CH node in LOCK, it must re-key. BS has selected the new CH. After a new chairman has been elected, CH distributes the new keys to its members using the Key Generation Node (KGN). This requires more energy. The AKE restarts the key process for establishing the finish of key life and the consumption of energy is extraordinary. In AKE, when a node enters into a network, a description is sent to BS. This communication is conveyed via the cluster which needs additional above contact. This overall contact uses further energy in the entire network. Meanwhile the CHs cannot detect compromised in time, their substation IDs must be reset and keys restored using their nearer CH through BS. Because of the CHs. Fuel is also used for additional purposes. Four, the resilience effect was calculated in a network of 500 nodes when 25 attack numbers were present, and the number of nodes resistance successfully.

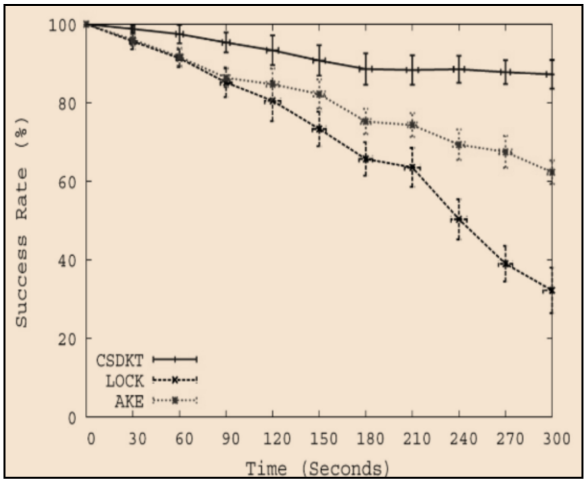

Figure 4: Network Success Rate with 25 Static Attackers.

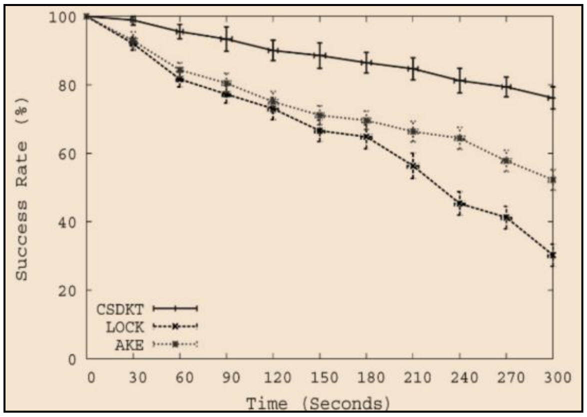

Figure 5: Network Success Rate with 25 Mobile Attackers.

For figures 4 & 5, there are two attacking cases. CBSDKT notices malicious network nodes and removes them. The malicious nodes do not engage in network activities, by comparison. The attackers don't even control nodes; the entire network can't change since the key changes dynamically in the next session based on variations in the components of the CCV. The attackers will therefore find it difficult to reach nodes.

CBSDKT accounts for approximately 88% of live nodes and is secure, because wholly malicious nodes are detected and removed from the network. The re-keying method is started in LOCK simply if the Node Capture is closer to the Resilience Point (Nc). The nodes are influenced by the network until they are re-keyed. In addition, the attackers are using the affected nodes to compromise the rest of the network nodes. It quickly decreases the proportion of living nodes. There is ability in AKE to collect the data-cache or pre-distributed cluster key in each node. After capture of these keys, the attackers will further attempt to compromise additional nodes before AKE restarts rekeying. AKE supports mobility, so that every attacker node's neighbour node changes to alternative cluster and achieves better than LOCK.

6. Conclusion

This section summarizes the safe mobility alert dynamic keying method for authentication in WSN. Our proposed method for security system can be applied for medium scale to large scale mobility aware applications that require the security at modest level. To provide the service for the WSN users along with the mobile nodes, the dynamic clustering has been performed. The CH model is chosen based on the weight determined by the ND, Dav, Sav, and VBP parameters. To order to ensure security, the CH uses authenticated key management systems if the cluster member exits or enters the network. The cluster members ' nodes re-select the CH when the CH usually leaves the network. The integrity and authentication for the data inside the network have been provided using the dynamic key which could not be easily predicted by the attackers. Since the keys are generated dynamically, the scalability is not an issue in this scheme. In addition to this, a two-way malicious node detection system is also castoff to delete malicious nodes and malicious CHs. Simulation proves that both inside and outside threats are avoided by the proposed system. Through growing the number of nodes, the amount of attackers and the amount of rounds, the proposed system is proof that efficient security is assured through reducing energy consumption, above regulation and packet loss. The proposed system also performs well in comparison with AKE and LOCK during high mobility. This work provides a chance to recognize complex keys that will be solved in the further analysis if a malicious node overhears the VBP or CCV values.

References

1. Amara, Said Ould, Beghdad, Rachid, and Oussalah, Mourad, Securing Wireless Sensor Networks: A Survey. EDPACS: The EDP Audit, Control and Security Newsletter, **47** (2) (March 06, 2013), 6-29.
2. Azarderskhsh, Reza and Reyhani-Masoleh, Arash, Secure Clustering and Symmetric Key Establishment in Heterogeneous Wireless Sensor Networks. EURASIP Journal on Wireless Communications and Networking, **2011** (2011), 12 pages.

3. Banihashemian, Saber and Bafghi, Abbas Ghaemi, A new key management scheme in heterogeneous wireless sensor networks. In Advanced Communication Technology (ICACT), 2010 The 12thInternational Conference on (Phoenix Park 2010), IEEE, 141 - 146.
4. Bellazreg, Ramzi and Boudriga, Noureddine, DynTunKey: a dynamic distributed group key tunneling management protocol for heterogeneous wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, **2014:9** (2014), 19 pages.
5. Boubiche, Djallel Eddine and Bilami, Azeddine, Cross Layer Intrusion Detection System For Wireless Sensor Network. International Journal ofNetwork Security & Its Applications (IJNSA), **4** (2) (March 2012), 35-52.
6. Boujelben, M, Cheikhrouhou, O, Youssef, H, and Abid, M, A Pairing Identity based Key Management Protocol for Heterogeneous Wireless Sensor Networks. In Network and Service Security, N2S '09. InternationalConference on (Paris 2009), IEEE, 1-5.
7. Boulis, Athanassios, Castalia: A simulator for Wireless Sensor Networks and Body Area Networks. NICTA. 2011.