Cluster Head Authentication Technique against Hello Flood Attack in Wireless Sensor Networks

Rupinder Singh
Research Scholar,
IKG PTU, Kapurthala, Punjab

Jatinder Singh, PhD
IKG PTU,
Kapurthala, Punjab

Ravinder Singh, PhD
IKG PTU,
Kapurthala, Punjab

ABSTRACT

The need for more effective security mechanisms is increasing with the growth of Wireless Sensor Network applications in different fields as there is an increase in the number of attacks that can be launched on them. Hello flood is one of such attack in the network layer of wireless sensor network in which an attacker with high transmission power can send or replay hello packets which are used for neighbor discovery. In this way, the attacker creates an illusion of being a neighbor to other sensor nodes and underlying routing protocol can be disrupted, which facilitate further types of attacks. The attacker broadcast packets with such a high power that a large number of sensor nodes in the network choose it as the parent node. In this paper, a novel technique based on RBG color cube number, an ID, and a unique Armstrong number is proposed for the authentication of a sensor node to become cluster head. The proposed technique is implemented in NS2, the experimental results clearly indicate the proposed technique has significant capability for the detection of hello flood attack launched for making the malicious node as the cluster head**.**

Keywords

Wireless sensor networks, Hello flood attack, RBG color cube, Armstrong number, Cluster head.

1. INTRODUCTION

Wireless Sensor Network (WSN) is defined as a self-configured and infrastructure-less wireless networks which is used to monitor environment or physical conditions, such as sound, temperature, humidity, wind direction, pressure, illumination intensity, chemical concentrations, speed, vibration intensity, power-line voltage, sound intensity, pollutant levels and so on. WSNs cooperatively pass the data gathered through the sensors to a centre location or sink (also called base station). This data is analyzed for further processing so as to take different decisions. Figure 1 shows the structure of a typical WSN. Sensor nodes in a WSN are inherently resource constrained and are vulnerable to various attacks due to the limited capacity of data processing speed, storage, communication bandwidth etc. The complexity of the implemented security algorithms also adds to the difficulty of providing security to WSNs. The past proposed security schemes for WSNs assumed that almost all nodes are trustworthy and cooperative, but the same is not true for most of the cases for many sensor network applications today. A large number of attacks are possible in WSN including jamming, tampering, exhausting, hello flood, collision, sinkhole, Sybil, denial-of-service, flooding, cloning etc.

Hello packets in WSN are used for neighbor discovery; a malicious node with high transmission power can send or replay these hello packets in order to launch hello flood attack. A number of countermeasures against Hello flood attack in WSN have been proposed in the literature that was discussed in our previous work [1]. Most of the proposed countermeasures have limitation and need improvement for producing more efficient one. In this paper, a novel technique based on RBG colour cube number, unique ID, and Armstrong number is proposed to authenticate the elected CH so as to prevent the WSN from hello flood attack. The remaining paper is organised as follows: In section II the hello flood attack in WSN is described. Section III describes cluster formation in WSN. In section IV, our proposed technique is discussed and in section V the simulation results are provided to show the effectiveness of the proposed technique. The paper ends with a conclusion in section VI.

2. HELLO FLOOD ATTACK

Hello flood attack is a network layer attack in WSN and is caused when hello packets used for neighbor discovery are sent or replayed by an attacker with high transmission power. In this way, the attacker creates an illusion of being a neighbor to other sensor nodes so that the underlying routing protocol can be disrupted, which smooth the progress of launching further types of attacks. The attacker broadcast packets with such a high transmission power that a large number of sensor nodes in the WSN choose it as the parent node or cluster head (CH) in the case of clustered implementation. Figure 2 shows the scenario of hello flood attack. All messages to be broadcasted in the WSN are routed through this parent sensor node that increases delay. The attacker broadcast these hello messages to a large number of sensor nodes in a wide area of the WSN. These sensor nodes are then forced to be convinced that the attacker node in the network is their neighbor. All the sensor nodes are going to reply to this HELLO message from the attacker and are going to waste their energy. This usually results in a confusion state in the WSN. Figure 3 and 4 show hello flood attack in the WSN. In this diagram circles, rectangle, and the triangle represents sensor nodes, base station, and attacker respectively.

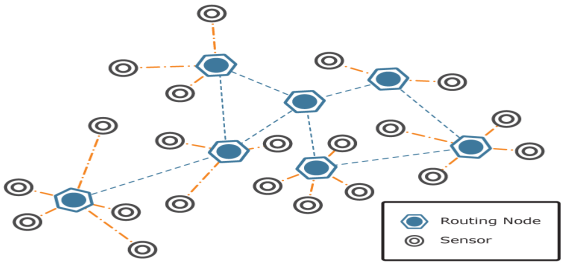


Figure 1: A typical WSN

In Hello flood attack advisory broadcast hello messages in WSN by capturing a sensor node and declare itself their neighbour. When any sensor node in the WSN receives this hello message, it assumes that sender node is in the communication range and starts communicating that sensor node and makes the entry in its routing table as a neighbor.

All sensor nodes in WSN communicate with BS through their neighbours. When an attacker node captures a legitimate node in the network or creates a fake node, it broadcast hello message to all nodes in the sensor network with the high power, it creates confusion to other sensor nodes that the message is coming from its neighbor nodes. So, all the nodes in the sensor network assume that the hello message path is the shortest path from the CH by assuming that attacker node (malicious) is a CH and starts communicates with the attacker. In this way, an attacker can control the cluster in the sensor network as the contact of sensor nodes is cut from the base station in the WSN and this also affects its routing. In this, an attacker makes use of Hello flood attack to become the CH in the WSN.

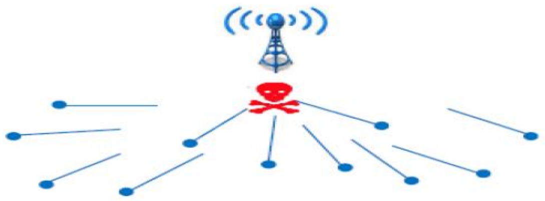
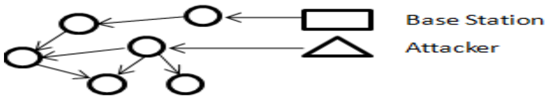


Figure 2: Hello Flood Attack



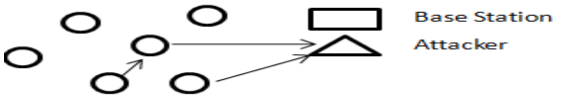


Figure 3: Shows broadcasting of hello packets by the attacker with more transmission power than a base station.

Figure 4: shows legitimate nodes considering attacker as their neighbours.

2.1 Properties of hello packet

C. Venkata et al. [2] describe the five main features of the Hello packet as given below:

1. The size of the Hello packet is smaller as compared to the data packet.
2. The probability of hello packet reaching to its receiver is usually higher than data packet especially in weak links in the network.
3. Broadcasting of the hello packet is done at basic bit rate since lower bit rate transmission is more reliable as compared to others.
4. Hello, packets do not require any acknowledgement for broadcasting.
5. Bidirectional communication of hello packets is not guaranteed.

2.2 Hello flood attack supporting attacks

1. A large number of other attacks are also supported by Hello flood attack including tempering, flooding, node capturing, false node replication etc. These supporting attacks are explained below:

1) Flooding: In flooding attack, the attacker continuously sends a new connection request to their neighbor in order to capture the resources. This results in severe resource constraints for legitimate nodes.

2) Tempering and node capturing: Tampering is the concern with attacks on components that involve modification of the internal structure of a single chip. An advisory can easily capture it and can be used for hello flood attack. Node capture attacks give the attacker full control over a sensor node, but node capturing is not easy. To do node capturing, attacker requires expert knowledge along with costly equipment and other resources. The difficulty is the removal of sensor nodes from the network for a large amount of time.

3) False node replication: In false node replication attack, a new sensor node is implanted by an attacker in the WSN by using the ID of a legitimate user. The attacker first removes the legitimate node from the network and at that place deploy false one. This false node replication can cause a huge destruction in WSN by supporting the Hello flood attack. An attacker can have control on the overall network for most of the time and therefore the damage occur from this attack is very high.

3. CLUSTERING IN WSN

In most of the WSN applications, it is required that the entire network must have the ability to operate in unattended harsh environments. In such environments, pure human access and monitoring may not be possible. Sensor nodes are deployed randomly by relatively uncontrolled means in the area and they usually form a network in an ad- hoc manner. Moreover, considering the entire area to be covered, it's a natural possibility that a large (hundreds) or even thousands of sensor nodes are to be involved. Sensor nodes in such environments are very energy constrained and their batteries regularly cannot be recharged. Therefore, the specialized energy-aware routing protocols offering required scalability should be implemented in the sensor network so that network's lifetime is preserved.

So, it is required that the sensor nodes should be grouped into clusters. This is needed in order to satisfy the scalability objective of WSN along with high energy efficiency condition for long network existence in large scale WSN environments. In the hierarchical structured sensor network, each cluster has a finite number of sensor nodes called members nodes and a chief node called CH. This CH usually performs the tasks of fusion and aggregation. The cluster formation process leads to a two-level hierarchy in the WSN where the CH sensor nodes form the higher level and the cluster member nodes form the lower level. The member nodes normally transmit their data to the corresponding CH nodes. The CH nodes in the WSN aggregate the data and transmit them to the BS either directly or through the midway communication with other CH nodes. As the CH nodes send all the collected data to higher distances as compare to the member sensor nodes, they spend energy at higher rates. One of the solutions for balancing this energy consumption among all the sensor nodes in a cluster is to regularly re-elect new CHs i.e. role of CH is rotated among capable sensor nodes. An example of the hierarchical data communication within a clustered WSN with single-hop intra-cluster communication and multi-hop inter-cluster communication is illustrated in figure 5.

The BS of the WSN is the central data processing point for the data received from the CHs. BS provides this data accessibility to the end users. BS is usually fixed and is at a faraway distance from the sensor nodes. The CH nodes usually act as gateways between the sensor nodes and BS. BS and CH act as the sink for the CH nodes and member nodes respectively. This structure formed between the BS, CH, and the sensors nodes can be replicated as many times as it is needed, creating multiple layers of the hierarchical WSN. The CH sensor nodes in the WSN are formed by some proposed algorithms for heterogeneous environments and can be pre-assigned. In most of the cases, however, the CHs are chosen from the deployed set of nodes either in a completely random way or probabilistic or based on other more specific criteria (connectivity, residual energy, etc.).

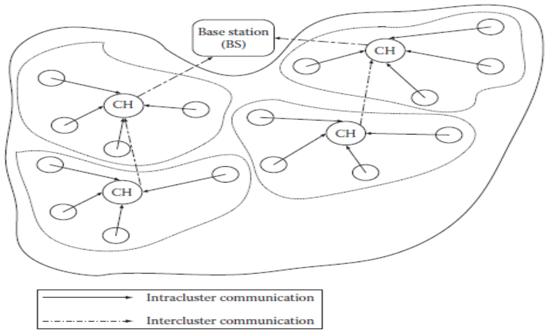


Figure 5: Clustered sensor network

4. AUTHENTICATED CLUSTER HEAD SELECTION

After the deployment of the sensor nodes, first clusters are formed in order to facilitate the energy-efficient communication. After the cluster formation, the entire network operation is divided into a number of rounds with each round consisting of three phases as shown in Figure 6.

They are Synchronization inside Cluster phase, Authenticated CH Election phase, Data Aggregation and Forward phase. In this work, the only focus is on the phase of the Authenticated CH Election. A CH selection scheme should satisfy the following conditions:

- Unpredictability - It should be impossible for a sensor node to predict which node will be elected as a CH.
- Non-manipulability - Any sensor node should not be able to modify a CH election result for its own benefit.
- Agreement property - All sensor nodes in a cluster should get the same election result.

It is assumed that the election of a CH is on the basis of a common random value. After the generation of a common random value, all cluster members in the WSN agree with a CH role node using this common value. All the members of a cluster contribute to the process of generating of the common random value by distributing their own random value. All members in the cluster generate aggregate random values and any other node cannot predict this value. A compromised sensor node can guess the common value by delaying its random value until all other members distribute their random values. The compromised sensor node can violate the condition of non-manipulability by avoiding its transmission i.e. if the compromised sensor avoids transmitting its random value, the CH election result is changed as the common value is changed. The transmission power of normal sensor nodes depends on the greatest hop distance also called cluster diameter between sensor nodes in the cluster. Malicious nodes can make several common values by lessening the signal transmission power when they transmit their random value in order to violate the agreement property of election results of a CH.

The CH formation also depends on the signal strength with which a sensor node broadcast hello message. The sensor node with more signal strength is expected to have more battery backup and likely to become CH. But, the intruder can broadcast a powerful hello message to all the nodes in the network as it has a huge power backup and hence, every node is likely to choose it as the CH. The CH election depends on both the signal strength and the random values so that a malicious node does not get elected. Still, there are chances of a malicious node to manipulate both of the above conditions so there is a need for strong CH authentication methodology. Here, the proposed secure CH selection technique is discussed for WSNs.

In the RGB color system (figure 7), each of the colors is defined by the amount of red, green and blue color that composes it. Most of the digital files make use of integer numbers between 0 and 255 in order to specify these quantities. The RGB color cube displays smooth transitions between these colors. It has 8 bits per components and 256*256*256 number of possible colors. An Armstrong number is an m-digit base n number such that the sum of its (base n) digits raised to the power m is the number itself. For example number 371 is an Armstrong number as $3^3+7^3+1^3$ =27 + 343 +1 = 371 which is equals to number itself. During the formation of the cluster, each sensor node is given a unique RBG color cube number, unique ID, and a unique Armstrong number by BS. This information is stored by BS in the registration table. After a sensor node in the WSN is elected as CH, before functioning it has to take permission from the BS. The BS ask for above information and verifies it from the registration table along with remaining energy level of the sensor node before it can be granted the status of CH. The flow chart in figure 8 illustrates our proposed methodology of selecting a CH in a secure way.

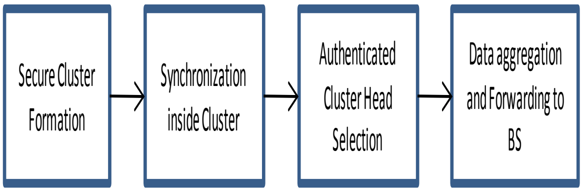

Secure Cluster Formation
Synchronization inside Cluster
Authenticated Cluster Head Selection
Data aggregation and Forwarding to BS

Figure 6: Operation of the sensor network

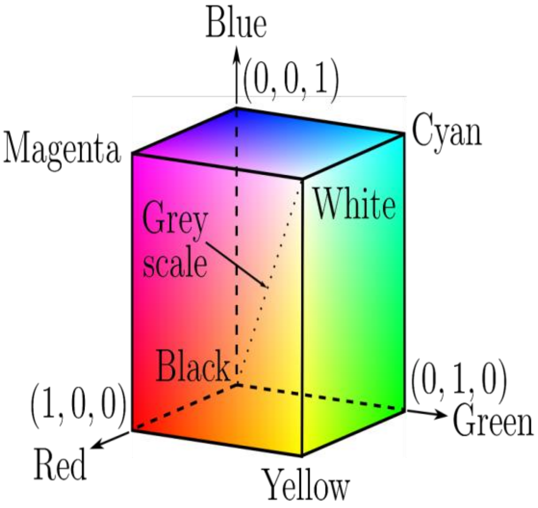


Figure 7: RBG color cube

5. SIMULATION RESULTS

In this section of the paper, the results of the simulation presented to show the effectiveness of proposed scheme. The simulation is carried out in ns2.35 with the parameters shown in table 1 below.

Table 1: Simulation parameters

Parameter	Value
Simulator used	NS 2.35
Area (meter)	800X800
No. of nodes	38
Routing protocol	LEACH
Channel type	Wireless
Packet size	512 byte
Mobility model	Two ray ground propagation model

5.1 Throughput

In the first experiment, sensor network throughput measured as this is one of the crucial network parameters. Network throughput refers to the average rate of successfully delivered packets. Throughput is calculated depending on a total number of packets received at the destination in sensor network per unit of time. Throughput is calculated as

Throughput = (Total number of packets received at the destination) / (simulation time)

Figure 9 shows the throughput analysis in the case of the sensor network without Hello flood attack, under Hello flood attack, and after implementation of proposed technique. The figure clearly shows that the proposed technique after the isolation of the Hello flood attack results in the increase of throughput.

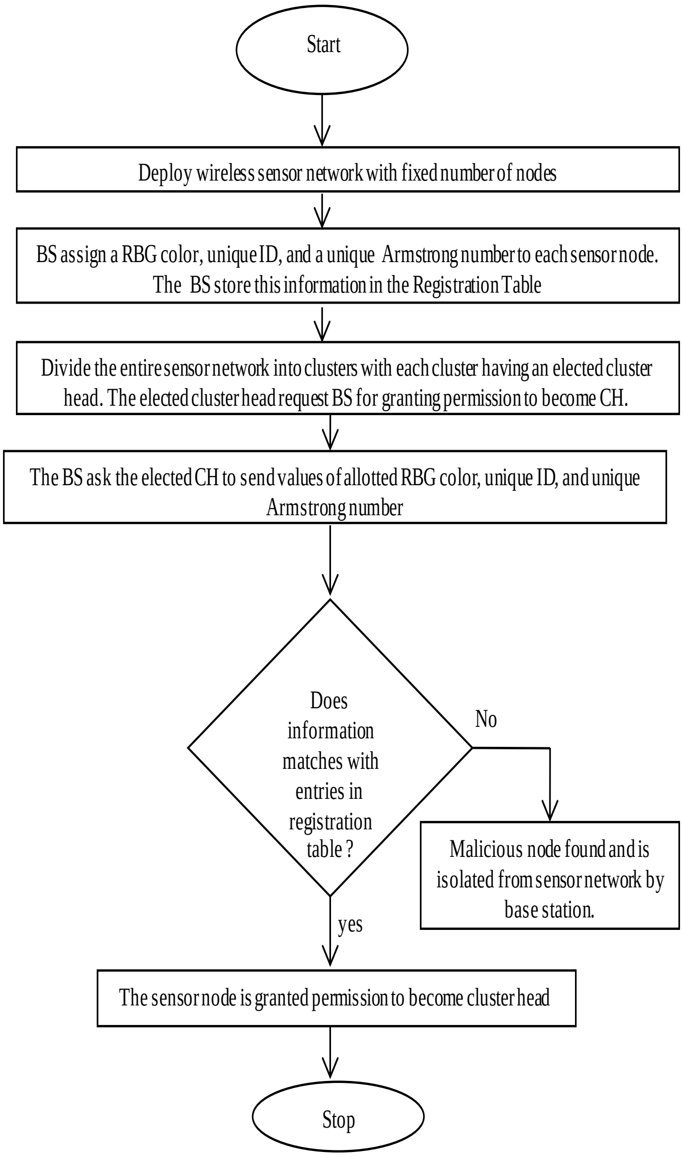

Start
Deploy wireless sensor network with fixed number of nodes
BS assign a RBG color, unique ID, and a unique Armstrong number to each sensor node. The BS store this information in the Registration Table
Divide the entire sensor network into clusters with each cluster having an elected cluster head. The elected cluster head request BS for granting permission to become CH.
The BS ask the elected CH to send values of allotted RBG color, unique ID, and unique Armstrong number
Does information matches with entries in registration table ?
No
Malicious node found and is isolated from sensor network by base station.
yes
The sensor node is granted permission to become cluster head
Stop

Figure 8: Flow chart of proposed detection technique

5.2 Packet delivery ratio

Packet delivery ratio (PDR) of a network is defined as the ratio of the total received packets at the destination to total packets generated by the source node. PDR is calculated as

PDR = (Packets received/packets generated) * 100

Figure 10 shows the PDR analysis in the case of the sensor network without Hello flood attack, under Hello flood attack, and after implementation of proposed technique. The figure clearly shows that the proposed technique after the isolation of the Hello flood attack results in the increase of PDR. A high value of PDR is an indication that there is less packet loss in the sensor network.

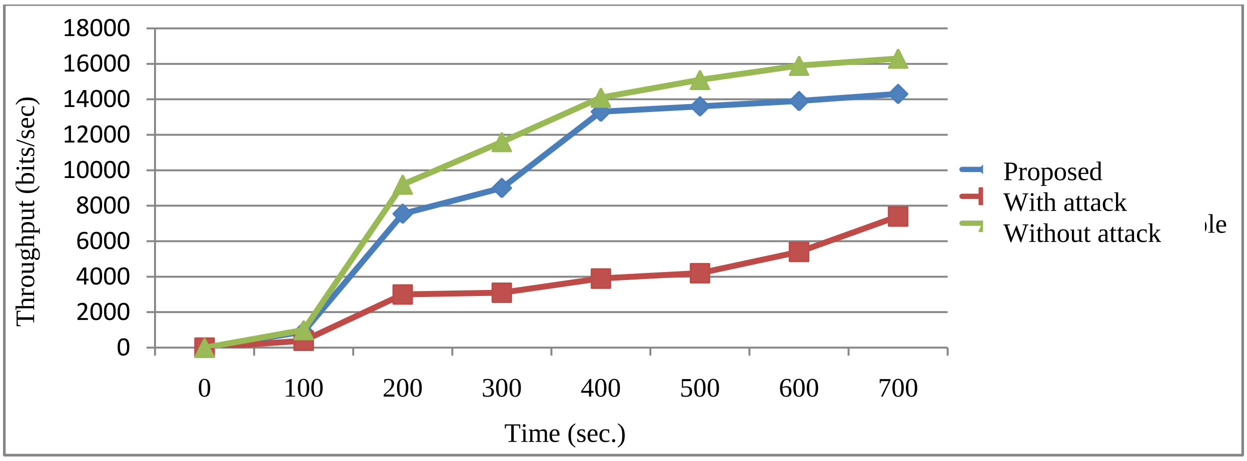


Figure 9: Throughput

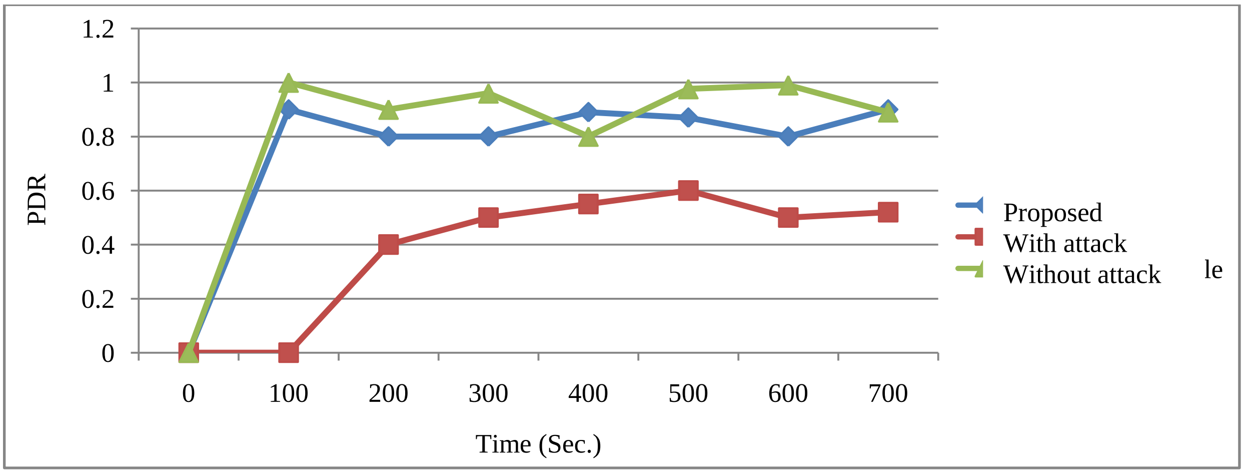


Figure 10: PDR

5.3 Delay

The delay is defined as the average time taken by a packet (data) to arrive at the destination. The delay also includes any delay that is caused by the process of route discovery along with queue in data packet transmission. The data packets successfully delivered to the destinations are only counted. It is calculated as:

Delay = ∑ (arrive time – send time) / ∑ Number of connections

The lesser value of delay is an indicator of the better performance of the protocol. Figure 11 shows the end to end delay in the case of sensor network without Hello flood attack, under Hello flood attack, and after implementation of proposed technique. The figure shows that the proposed technique results in the decrease in end-to-end delay.

5.4 Overhead

Overhead is the excess time taken by the protocol to deliver the packets to the destination. Hello flood attack increases the overhead in the sensor network. The routing overhead is defined as the count of packets used for routing in the sensor network. Figure 12 shows overhead in the case of sensor network without Hello flood attack, under Hello flood attack, and after implementation of proposed technique. The proposed technique results in decreasing the overhead of the network as shown in figure 12.

5.5 Energy consumption

For the energy computation of sensor nodes, an initial value of 10 joules is assigned at the beginning of the simulation. This energy is termed as initial energy. In the simulation, the variable energy is used to represent the energy level in a sensor node at any specified time. The value of the initial energy is passed as an input argument. A sensor node loses a specific amount of energy for every packet being transmitted and received. As a result of this, the value of initial energy in a sensor node gets decreased. The energy consumption level of a sensor node at any time of the simulation is determined by finding the difference between the current energy values

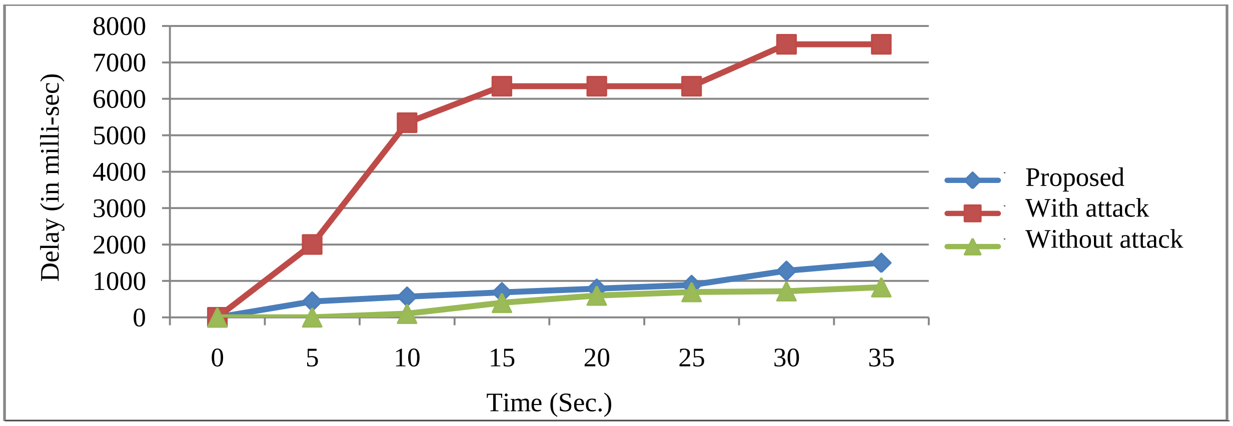


Figure 11: Delay

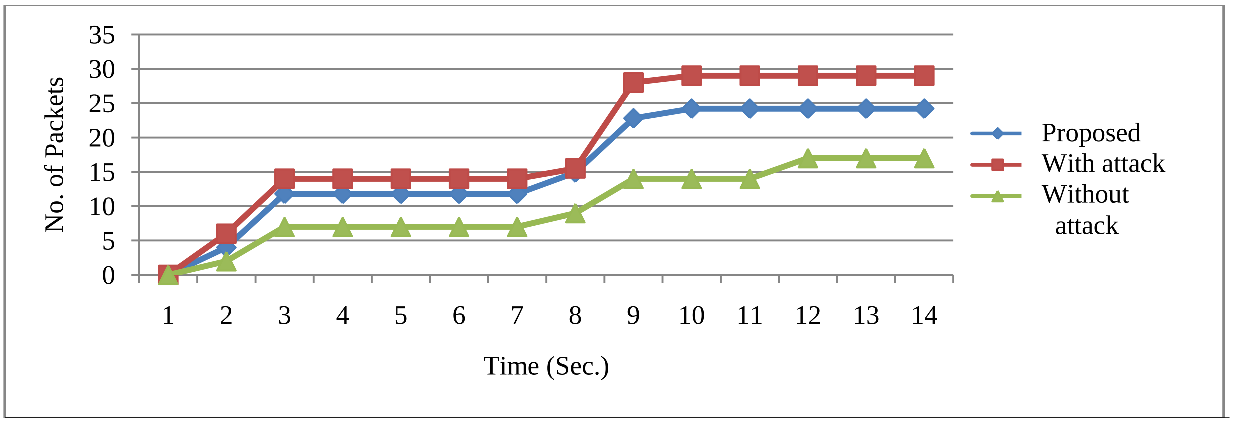


Figure 12: Overhead

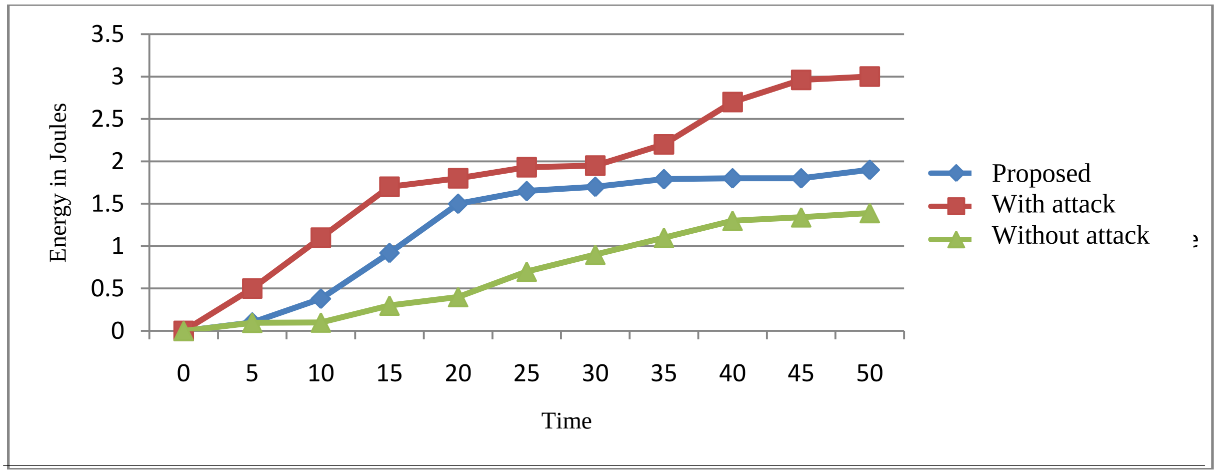


Figure 13: Energy consumption

and initial energy value. If an energy level of a sensor node reaches to zero, it cannot transmit or receive any more packets. Figure 13 show the proposed technique reduces the energy consumption as compared to the attacked scenario of the sensor network.

6. CONCLUSION

The secure selection of cluster head in the clustered wireless sensor network is crucial as all the cluster sensor members data to the base station is communicated through cluster head. Hello flood attack can be used for making a cluster head compromised in which malicious sensor node with high transmission power can send or replay hello packets which are used for neighbor discovery. In this paper, the procedure for the election of cluster head depending on both the signal strength and the random values is presented so that a malicious node does not get elected. Then, a novel technique based on RBG color cube number, an ID, and a unique Armstrong number is proposed to authenticate the elected cluster head. The proposed approach improves the WSN performance by early detection of the adversary and preventing the nodes from associating with such a malicious cluster head. Our cluster formation methodology generates large sized clusters. The simulation results represent that our scheme expels compromised nodes from clusters and results represent that our scheme raises the quality of clusters and more energy-efficient than a rival scheme. The implementation of the proposed technique in NS2 shows its efficiency for the factors of throughput, packet delivery ratio, delay, overhead, energy consumption. The additional simulation will be done in the future by increasing the number of sensor nodes. The proposed technique will also be compared with existing one to show the efficiency level of the scheme.

7. ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

8. REFERENCES

[1] Rupinder Singh, Dr. Jatinder Singh, and Dr. Ravinder Singh, “Hello flood attack Countermeasures in Wireless Sensor Networks”, International Journal of Computer Science and Mobile Applications, Vol. 4, Issue 5, April 2016, pp. 1-9.

[2] C. Venkata, Mukesh Singhal, James Royalty, and Srilekha Varanasi, “Security in wireless sensor networks”, Wireless communications and mobile computing Published online in Wiley Inder Science, 2006

[3] Yaya Shen, Sanyang Liu, Zhaohui Zhang, “Detection of Hello Flood Attack Caused by Malicious Cluster Heads on LEACH Protocol”, International Journal of Advancements in Computing Technology (IJACT), Volume 7, Number 2, March 2015.

[4] Gayatri Devi, Rajeeb Sankar Bal, Nibedita Sahoo, “Hello Flood Attack Using BAP in Wireless Sensor Network”, International Journal of Advanced Engineering Research and Science, Vol. 2, Issue 1, ISSN: 2349-6495, Jan. 2015.

[5] S. Mayur, H. D. Ranjith, “Security Enhancement on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, ISSN (Online): 2319 – 8753, ISSN (Print): 2347 – 6710, March 2015.

[6] S. Rawan, M. Suhare, A. Manal, “Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme”, International Journal of Computer and Communication Engineering, Volume 4, Number 3. May 2015.

[7] Dilpreet Kaur, Rupinderpal Singh, “Energy level based Hello Flood attack Mitigation on WSN”, International Journal of Embedded Systems and Computer Engineering, ISSN 23213361, July 2015.

[8] Jyoti, Ashu Bansal, “Detection of Hello Flood Attack on Leach Protocol Based on Energy of Attacker Node”, International Journal of Innovations & Advancement in Computer Science, Volume 4, ISSN 2347 – 8616, September 2015.

[9] Shikha Magotra, Krishan Kumar, “Detection of HELLO flood Attack on LEACH Protocol”, IEEE International Advance Computing Conference (IACC), 2014.

[10] J. Steffi, Agino Priyanka, S. Tephillah, and A. M. Balamurugan, “Attacks and countermeasures in WSN”, International Journal of Electronics & Communication, Volume 2, Issue 1, ISSN 23215984, January 2014.

[11] Satwinder Kaur Saini, Mansi Gupta, “Detection of Malicious Cluster Head causing Hello Flood Attack in LEACH Protocol in Wireless Sensor Networks”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 5, ISSN 2319 – 4847, May 2014.

[12] Akhil Dubey, Deepak Meena, Shaili Gaur, “A Survey in Hello Flood Attack in Wireless Sensor Networks”, International Journal of Engineering Research & Technology (IJERT), Vol. 3, Issue 1, ISSN: 2278-0181, January 2014.

[13] Virendra Pal Singh, S. Aishwarya, Anand Ukey, and Sweta Jain, “Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks”, International Journal of Computer Applications, Volume 62, No.15. January 2013.

[14] Nusrat Fatema, Remus Brad, “Attacks and counterattacks on wireless sensor networks”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol. 4, No. 6. December 2013.

[15] A. Anup wanjari, Vidya Dhamdhere, “Evading Flooding Attack in MANET Using Node Authentication”, International Journal of Science and Research (IJSR), Volume 3, Issue 12, ISSN (Online): 2319-7064, December 2014.

[16] Mohammad Sayad Haghighi, Kamal Mohamedpour, Vijay Varadharajan, and Barry G. Quinn, “Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks”, IEEE transactions on information forensics and security, Vol. 6, No. 4, December 2011.

[17] Virendra Pal Singh, Sweta Jain, and Jyoti Singhai, “Hello Flood Attack and its Countermeasures in Wireless Sensor Networks”, International Journal of Computer Science Issues, Vol. 7, Issue 3, No. 11, ISSN 1694-0814, May 2010.

[18] Mohamed Osama Khozium, “Hello Flood Counter Measure for Wireless Sensor Network”, International Journal of Computer Science and Security, Volume 2, Issue 3, May 2008.

[19] A. Hamid, Mamun Rashid, Choong Seon Hong, “Defense against lap-top class attacker in wireless sensor network”, The 8th International Conference Advanced Communication Technology, Print ISBN: 89-5519-129-4, IEEE, 2006.

[20] Waldir Ribeiro Pires J´ unior Thiago H. de Paula Figueiredo Hao Chi Wong, “Malicious Node Detection in Wireless Sensor Networks”, 18th International Parallel and Distributed Processing Symposium, Print ISBN:0-7695-2132-0, IEEE, 2004.

[21] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, “A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN”, International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[22] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, “A Cross-Layer Based Intrusion Detection Technique for Wireless Networks”, The International Arab Journal of Information Technology, Vol. 9, No. 3. May 2012.