Indian Journal of Science and Technology, *Vol 10(13), DOI: 10.17485/ijst/2017/v10i13/99503, April 2017* *ISSN (Print) : 0974-6846*
ISSN (Online) : 0974-5645

To Propose a Novel Technique for Detection and Isolation of Dictionary Attack in Wireless Sensor Network

Supreet Kaur

Department of Computer Science and Engineering, Chandigarh University, Mohali – 140413, Punjab, India;
smilyindia1992@gmail.com

Abstract

Objectives: The main objective of this work is to isolate dictionary attack in wireless sensor networks. In the existing techniques Diffie-Helman algorithm has been proposed for the secure channel establishment from source to destination. In the Diffie-Helman algorithm dictionary attack is possible which reduce network performance. In this work, ECC technique is used which will detect malicious nodes from the network. **Methods/Statistical Analysis**: The wireless sensor networks are the kind of network in which sensor nodes can sense natural conditions and it is conveyed to the far spots like a backwoods, deserts and so on. Wireless sensor networks have faced various kinds of issues and challenges out of which maintaining the maintenance of security has proven to be one of the greatest concern. There has been a higher probability of occurrence of an attack due to all such problems related to security. All such discussions related to wireless sensor networks have been made in this paper. Wireless sensor networks have self configuring nature which results in dictionary attack is possible in the network. The delay and energy consumption get an increment as a result. The throughput of the network also gets affected as it gets reduced. Henceforth, for the purpose of detecting and isolating these dictionary attacks, a new technique has been put forth. The proposed technique is based on Elliptic Curve Cryptography (ECC), in which digital signature is calculated not which do not satisfy the condition of signature can be marked as malicious. **Findings:** In the existing technique to establish secure channel from source to destination, Diffie-Helman algorithm has been proposed in which secure session key is established. Due to self configuring nature of WSN dictionary attack is possible in the network. The ECC technique is used to ensure data integrity in the network. In the ECC technique, digital signature is generated as the source end and that digital signature is verified at the destination end. If the signature is not verified at the destination, then intrusion is detected in the network. To detect malicious node data integrity is confirmed per hop and the nodes which do not satisfy the condition of digital signature are detected as the malicious node. The proposed method is implemented in MATLAB and it has been analyzed that the network performance is increased in terms of energy consumption, throughput and delay after detection of malicious nodes.

Keywords: Dictionary Attack, Diffie-Helman, ECC, Intrusion, WSN

1. Introduction

Wireless Sensor Network (WSN) comprises of different wireless sensor nodes where each hub is associated with one sensor or at some point with a few sensors. This sensor node is comprised of radio transceiver which keeps track of the completely associated network[1]. These sensor nodes are utilized to monitor the natural parameters. WSN has is not much complex and it has decentralized structure. In WSN, nodes measure the conditions in the environment surrounding them. These estimations are then changed into signal that can be created on the basis of various parameters. At that point the gathered information is sent to the sink. Further the sink sends

**Author for correspondence*

information to the client through certain communication mode. (Figure 1) indicates the data flows from sensor node V to node S through node M and a node N to sink or destination[2].

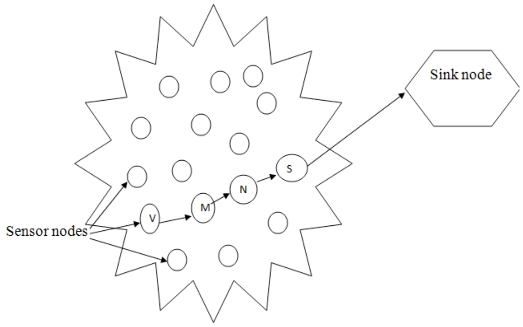


Figure 1. Wireless sensor network.

1.1 Stable Election Protocol (SEP)

There are various types of nodes which are present in the heterogeneous network which are used in the energy levels. The energy consumption is reduced with the help of clustering. The network lifetime of the network is increased. There are various types of protocols used in the methodology. Due to the non-productive nature of the batteries in nodes, the protocols of the networks are energy productive.

The Stable Election Protocol (SEP) is used in the heterogeneous networks which is a reactive directing method. The selection of cluster head in this cluster based routing protocol is done with the help of decision probability. The heterogeneous networks have the applications of this protocol. The execution of the network is dependent on the effective usage of the energy within the network. The nodes are broadly classified into two categories on the basis of the heterogeneous two level energy based WSN system. The categories are namely, the higher energy nodes which are known as the advance nodes and the lower energy nodes which are known as the normal nodes. It is made sure by the method that the cluster head selection is done from advance nodes more frequently as compared to that of the normal nodes. The stability time of the network is amplified with the help of this methodology[3].

The various kinds of transmissions provided in the wireless network system are not taken under consideration by the SEP during the application of clustering rule in the heterogeneous network. The kinds of transmissions involved are Intra Cluster Transmission, Inter Cluster Transmission as well as the Cluster Head to Base Station Transmission. All the transmissions occurring in the network are considered to be within the same class by the SEP. For each transmission, similar amount of energy is measured and distributed. This is not genuine for all kinds of applications or situations. The Intra Cluster Transmission's energy prerequisite is different from that of the Inter Cluster Transmission or from the cluster head to base station transmission[4].

1.2 Attacks in WSN

There can be number of malignant attacks which are confronted by remote sensor systems on Network layers which can be characterized as beneath:-

1.2.1 Cloning Attack

Clone attack[5] (likewise called node replication attack) is an extreme attack in WSNs. In this attack, an enemy gets only a few nodes, copies them and after that passes on an optional number of replicas all through the framework. The catch of nodes is possible in a way that sensor nodes are commonly unprotected by physically ensuring in view of cost examinations, and are consistently left unattended after arrangement. In case one doesn't perceive these replicas, the framework will be powerless against an immense class of insider attacks. For instance, the enemy now can catch the action passing the replicas (which may contain the after indicated ranges of officers), infuse false information into the system (which might be a false summons), slander distinctive nodes and even revoke legitimate nodes.

1.2.2 Sinkhole Attack

For the purpose of drawing all the traffic from a specific area with the help of a compromised node, the malicious node is used. The sinkhole which is metaphorical is made to be placed in the center. The compromised node is made to be shown as if it is engaged by the sinkhole attack. The node is made to look as if it is engaged in some computations. The information which is coordinated is provided by the nodes which make it difficult to identify the sinkhole attacks in the network. This attack has within it a high power radio transmitter which authorizes it such that the energy is transmitted for the purpose of achieving a huge framework[6] which is shown in (Figure 2).

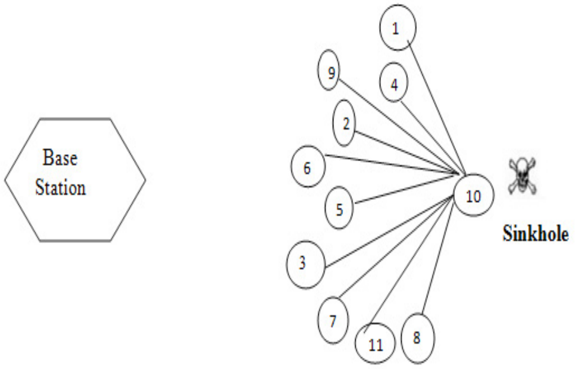


Figure 2. Sinkhole attack.

1.2.3 Wormhole Attack

In this, the attacker gets packets from one point in the system, advances them through a remote or wired link with low latency in the system. Along these lines, a default link is utilized by the attacker as a part of the system. With the assistance of this link, attacker transfers packet to another area in the system[7] as shown (Figure 3)

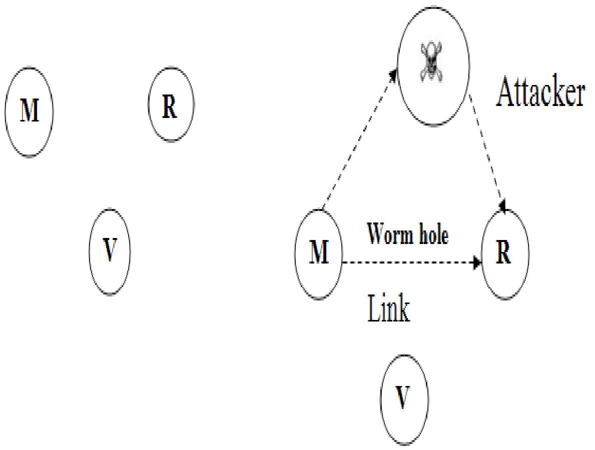


Figure 3. Wormhole attack.

1.2.4 Sybil Attack

This attack is a systematic risk presented by one or many malicious nodes to pronounce various unlawful recognizes to befuddle or even fall the system applications. A Sybil attack is an attack which makes different personalities from the same malicious node. In a Sybil attack, an attacker makes a few illegitimate personalities in sensor organizes either by manufacture or taking the characters of genuine nodes[8].

Authors[1] plan innovative Message observation Mechanism (MoM) to distinguish and safeguard the DoS attack. In view of the spatial-temporal correlation, MoM uses the similarity function to distinguish the substance attack and additionally the recurrence attack. The MoM receives rekey and reroute countermeasures to confine the malicious node. The DoS attack is verified and resisted by the security investigation. Along with this it can reduce the energy consumption. Another way to deal with accomplishing privacy is proposed[2] in multi-hop code, authors introduce the dissemination protocol. The DoS-attack resistivity and privacy are combined within a multi-hop code dissemination protocol in this paper. The Deluge is an open source application methodology and is used in the best class code dissemination protocol for the wireless networks. In this scheme, a performance assessment is provided and the comparisons are provided with the original and the new current secure Deluge scheme. Author[3] shows the handling of the malicious attacks in the proactive as well as the reactive protocols. It is checked whether one sort of protocol offers characteristically better resistance to the different attacks than the other. The author[4] portrays that we can overcome numerous dangers utilizing existing encryption and authentication mechanisms and different systems can ready network administrators of ongoing attacks or trigger procedures to preserve energy on influenced gadgets. The author[5] proposes Trust-Aware Routing Framework (TARF), a trust-aware routing framework for WSNs, to secure multi-hop routing in WSNs against gatecrashers misusing the replay of routing information with trust administration; TARF empowers a node to keep track of the trustworthiness of its neighbors and along these lines to choose a reliable course. Not just does TARF bypass those malicious nodes abusing different nodes personalities to mislead network traffic, it additionally achieves productive energy utilization. Authors[6] focus here on the security of WSN which provides certain conclusions. The security of huge frameworks ought to be persistently reassessed for considering new recognitions. The level of security required for the application ought to likewise be checked while inclining toward hardware. The author[7]addresses a particularly a very harmful sort of DoS attack called PDoS (Path-based Denial of Service) in which a foe overpowers sensor nodes a long separation away by flooding the node with replayed packets or injected spurious packets. An answer utilizing one-way hash chains to ensure end-to-end correspondences in WSNs against PDoS attacks is proposed. The arrangement gave is lightweight endures burst packet losses, and can without much of a stretch be executed in advanced WSNs. The author[8] has presented energy proficient three level clustering plan taking into account weighted probabilities for the decision of cluster heads[9]. This new protocol contrasts its performance and LEACH protocol in the nearness of heterogeneity. It has three sorts of nodes, super nodes, advanced node and normal node. Every node has diverse weight probabilities, taking into account these probabilities the threshold is acquired that is utilized to choose the cluster heads in each round[10]. It exploits heterogeneity by utilizing the additional energy of super node therefore diminishes the unstable region and expansions the stable region.

2. Dictionary Attack in WSNs

The challenge-response protocol is helpless against a password-guessing attack. In this kind of attack, it is expected that an adversary has effectively assembled a database of possible passwords, called a dictionary[11]. The adversary eavesdrops on the channel and records the transcript of a fruitful keep running of the protocol to take in the arbitrary challenge and response. At that point the adversary chooses passwords from the dictionary and tries to produce a response that matches the recorded one. On the off chance that there's a match, the adversary has effectively speculated A's password. After each failed matching endeavor, the adversary picks a different password from the dictionary and repeats the procedure[12]. This non-interactive form of attack is known as the offline dictionary attack. Here and there an adversary may attempt different user IDs and passwords to log in to a system. For mainstream Internet administrations like Yahoo!, the adversary can inconsequentially pick any sensible user ID because of the vast number of registered users[13]. An adversary can likewise find user IDs within interactive Web people group, for example, auction sites. In the event that the system rejects the password as being incorrect for that specific user, the adversary picks a different password from the dictionary and repeats the procedure. This interactive form of attack is known as the online dictionary attack[14].

3. Proposed Methodology

The WSNs are the sort of network in which sensor nodes are conveyed to sense ecological conditions like temperature, weight, pressure and so on. The sensor network is the decentralized kind of network because of which different sort of security attacks are conceivable in the network. The security attacks are conceivable on the grounds that some malicious nodes may join the network. In this work, range based node localization technique is proposed which will identify malicious nodes, which are capable of triggering Dictionary attack in the network[15].

3.1 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) has now gained widespread exposure and acceptance, and has ultimately moved from being an interesting mathematical construction to a well-established public-key cryptosystem already included in numerous standards and adopted by an increasing number of companies. ECC has a number of advantages over other public-key cryptosystems where the size of the cryptographic keys and operands are involved in the computation of EC cryptosystems as they are much shorter[16]. From the mathematical standpoint, an elliptic curve is the solution set to the bivariate polynomial equation

$$f(x,y) = \mathbf{0}\ ,$$

Where $f(x,y)$ is of total degree 3, and $f(x,y)$ is irreducible.

In cryptography particular equations and particular (finite) fields are considered over which curves are defined[17]. The points on the curve form a commutative group. Elliptic curves are particularly attractive for cryptographic applications because the discrete logarithm problem in elliptic curve groups is computationally hard. The implementation security and efficiency are the two important factors of ECC. The role of the implementation efficiency requirement is known as the possibility to achieve suitable levels of execution time, resources required, power consumed, costs, along with flexibility and reusability of design solutions. The implementation security however, generates a significant, perhaps crucial portion of the real security risk[18]

3.2 Procedure

The following strides are followed for the recognition of malicious nodes[19]:

1. Deploy WSNs with finite number of sensor nodes
2. Apply LEACH protocol for cluster entire network and in every cluster selects cluster head on the premise of distance and energy

3. Select shortest path from source to sink on the premise of reactive routing protocol
4. Apply technique of ECC to detect malicious nodes from the network
5. Isolate detected malicious nodes and re-build up the path from source to sink.

As portrayed in the flowchart (Figure 4), the network is deployed with the finite number of sensor nodes. The entire network is partitioned into altered size clusters. The shortest path will be built up from source to destination through the cluster heads. The ECC technique is connected which will identify malicious node from the network. The ECC technique will calculate digital signature and node which is changing the data will not able to calculate correct signature and that node will be detected as malicious node.

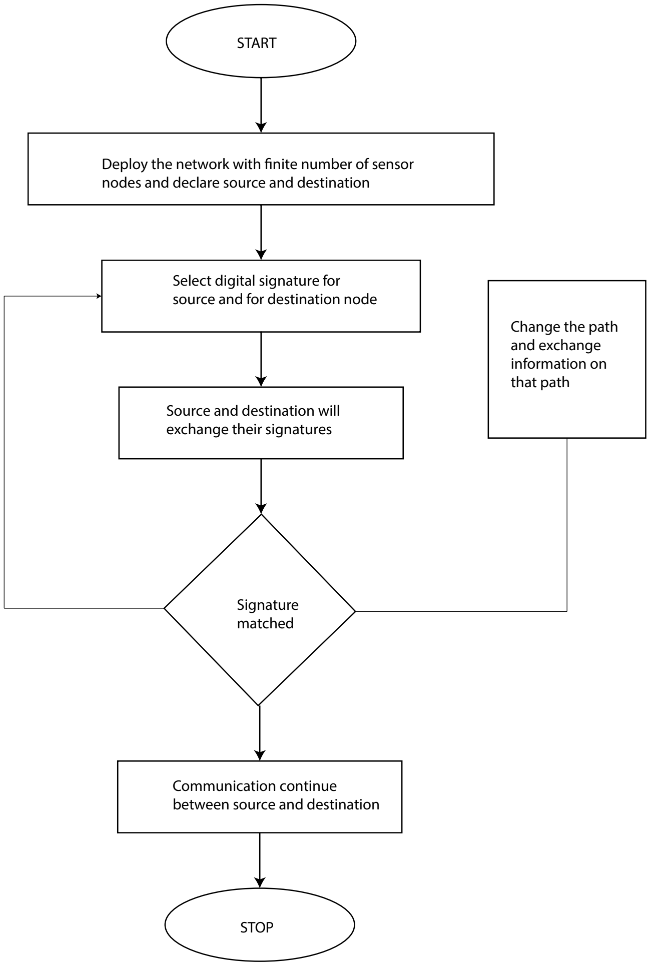
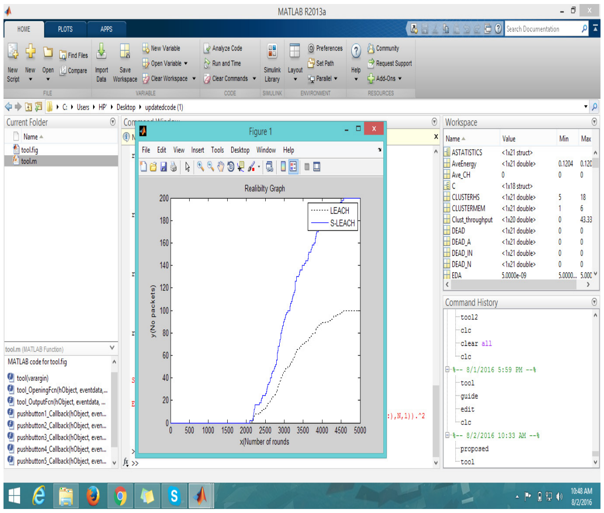

START
Deploy the network with finite number of sensor nodes and declare source and destination
Select digital signature for source and for destination node
Change the path and exchange information on that path
Source and destination will exchange their signatures
Signature matched
Communication continue between source and destination
STOP

Figure 4. Flowchart of proposed methodology.

As shown in (Table 1), the various parameters values which are used for the simulation. The simulation parameter represents the assumption which are considered while implementing the procedure

4. Experimental Results

In this work, node localization technique is applied to detect malicious node from the network. The novel technique is implemented in MATLAB.

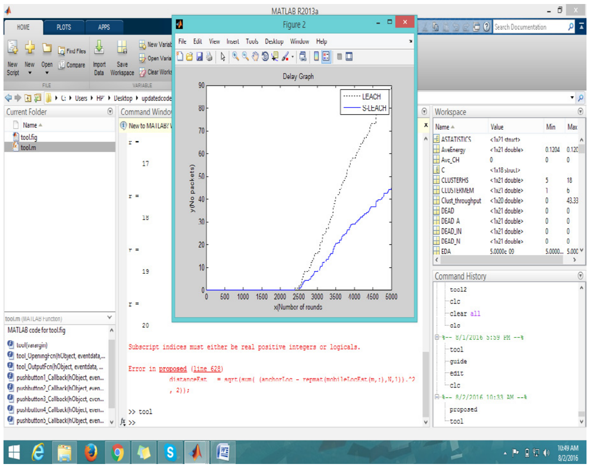


Name	Value	Min	Max
ASTATISTICS	<1x21 struct>		
AveEnergy	<1x21 double>	0.1204	0.120
Ave_CH	0	0	0
C	<1x18 struct>		
CLUSTERHS	<1x21 double>	5	18
CLUSTERMEM	<1x21 double>	1	6
Clust_throughput	<1x20 double>	0	43.33
DEAD	<1x21 double>	0	0
DEAD_A	<1x21 double>	0	0
DEAD_IN	<1x21 double>	0	0
DEAD_N	<1x21 double>	0	0
EDA	5.0000e-09	5.0000...	5.000

```
tool2
clc
clear all
clc
%-- 8/1/2016 5:59 PM --%
tool
guide
edit
clc
%-- 8/2/2016 10:33 AM --%
proposed
tool
```

Figure 5. Reliability graph.

As illustrated in Figure 5, the comparison of proposed and existing algorithm in terms of reliability. It is been analyzed that reliability of the improved algorithm is increased as compared to existing algorithm



```
r =

    17


r =

    18


r =

    19


r =

    20

Subscript indices must either be real positive integers or logicals.

Error in proposed (line 628)
        distanceEst   = sqrt(sum( (anchorLoc - repmat(mobileLocEst(m,:),N,1)).^2
        , 2));

>> tool
>>
```

Name	Value	Min	Max
ASTATISTICS	<1x21 struct>		
AveEnergy	<1x21 double>	0.1204	0.120
Ave_CH	0	0	0
C	<1x18 struct>		
CLUSTERHS	<1x21 double>	5	18
CLUSTERMEM	<1x21 double>	1	6
Clust_throughput	<1x20 double>	0	43.33
DEAD	<1x21 double>	0	0
DEAD_A	<1x21 double>	0	0
DEAD_IN	<1x21 double>	0	0
DEAD_N	<1x21 double>	0	0
EDA	5.0000e-09	5.0000...	5.000

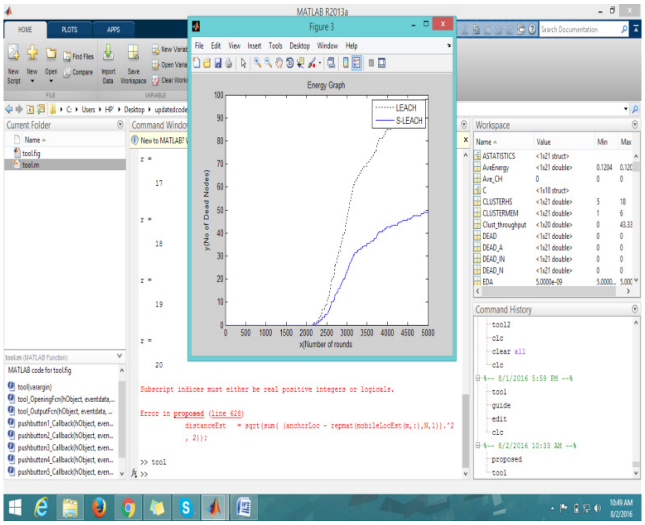
```
tool2
clc
clear all
clc
%-- 8/1/2016 5:59 PM --%
tool
guide
edit
clc
%-- 8/2/2016 10:33 AM --%
proposed
tool
```

Figure 6. Delay graph.

Table 1. Parameter table

Antenna type	Omi directional
MAC layer	802.11
Number of nodes	100
Link layer type	LL
Channel type	Wireless channel
Area	800*800

As shown in Figure 6, the efficiency of proposed and existing algorithm is compared in terms of delay and it is been analyzed that network delay is reduced when dictionary attack is isolated from the network

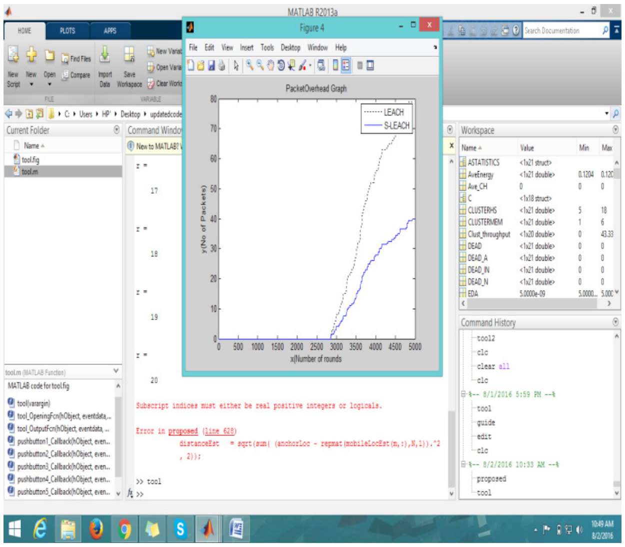


```
r =

    17


r =

    18


r =

    19


r =

    20

Subscript indices must either be real positive integers or logicals.

Error in proposed (line 628)
        distanceEst   = sqrt(sum( (anchorLoc - repmat(mobileLocEst(m,:),N,1)).^2
        , 2));

>> tool
fx >>
```

Name	Value	Min	Max
ASTATISTICS	<1x21 struct>		
AveEnergy	<1x21 double>	0.1204	0.120
Ave_CH	0	0	0
C	<1x18 struct>		
CLUSTERHS	<1x21 double>	5	18
CLUSTERMEM	<1x21 double>	1	6
Clust_throughput	<1x20 double>	0	43.33
DEAD	<1x21 double>	0	0
DEAD_A	<1x21 double>	0	0
DEAD_IN	<1x21 double>	0	0
DEAD_N	<1x21 double>	0	0
EDA	5.0000e-09	5.0000...	5.000

```
tool2
clc
clear all
clc
%-- 8/1/2016 5:59 PM --%
tool
guide
edit
clc
%-- 8/2/2016 10:33 AM --%
proposed
tool
```

Figure 7. Energy graph.



```
r =

    17


r =

    18


r =

    19


r =

    20

Subscript indices must either be real positive integers or logicals.

Error in proposed (line 628)
        distanceEst   = sqrt(sum( (anchorLoc - repmat(mobileLocEst(m,:),N,1)).^2
        , 2));

>> tool
fx >>
```

Name	Value	Min	Max
ASTATISTICS	<1x21 struct>		
AveEnergy	<1x21 double>	0.1204	0.120
Ave_CH	0	0	0
C	<1x18 struct>		
CLUSTERHS	<1x21 double>	5	18
CLUSTERMEM	<1x21 double>	1	6
Clust_throughput	<1x20 double>	0	43.33
DEAD	<1x21 double>	0	0
DEAD_A	<1x21 double>	0	0
DEAD_IN	<1x21 double>	0	0
DEAD_N	<1x21 double>	0	0
EDA	5.0000e-09	5.0000...	5.000

```
tool2
clc
clear all
clc
%-- 8/1/2016 5:59 PM --%
tool
guide
edit
clc
%-- 8/2/2016 10:33 AM --%
proposed
tool
```

Figure 8. Packet overhead comparison.

As shown in Figure 7, the energy comparison is shown between the proposed and existing algorithm and it is been analyzed that when attack is triggered in the network. When attack is isolated from the network energy consumption is reduced.

As shown in Figure 8, the compared in terms of routing overhead. The routing overhead is the parameter in which it is measured that how many number of extra packets get transmitted in the network. Due to dictionary attack in the network packet overhead is increased in the network. This is analyzed that packet overhead is reduced after isolation

5. Conclusion

WSN comprises of an application based structure which also consists of some challenges in it. When the network is implemented in various systems, it is prone to various types of attacks. The main ideology discussed in this paper is to identify and confine the dictionary attack. A technique has been put forth which comprises of distinguishing and disengaging the malicious nodes from the respective network. The ECC technique is applied to confirm malicious node. The nodes which can result in causing a dictionary attack are highlighted. At the end of the study, the performance analysis is made by checking certain parameters which rely upon delay, throughput as well as energy of the network.

6. References

1. Yi-Ying Z, Xiang-zhen L, Liu YA. The detection and defense of DoS attack for wireless sensor network. Journal of China Universities of Posts and Telecommunications. 2012 Oct; 19(2):52–6.
2. Hailun T, Diethelm O, Zic J, SanjayJha S. A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor network. In the Proceedings of the second Association for Computing Machinery (ACM) conference on Wireless network security, Zurich, Switzerland; 2009 Mar 16–19. p. 245–52.
3. Kumar S, Verma SK, Kumar A. Enhanced threshold sensitive stable election protocol for heterogeneous wireless sensor network. Wireless Personal Communications, Springer. 2015 Dec; 85(4):2643–56.
4. Raymond DR, Midkiff SF. Denial-of-service in wireless sensor networks: attacks and defenses. Institute of Electrical and Electronics Engineers (IEEE) Pervasive Computing. 2008 Jan – Mar; 7(1):74–81.

5. Guoxing Z, Weisong S, Julia D. TARF: a Trust-Aware Routing Framework for wireless sensor networks. European Conference on Wireless Sensor Networks (EWSN), Lecture Notes in Computer Science, Springer. 2010; 5970:65–80.
6. Hero M, Rosli S, Moravejosharieh A. Overview of security issues in wireless sensor networks. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) Third International Conference on Computational Intelligence, Modelling and Simulation; 2011 Sep 20–22. p. 308–11.
7. Jing D, Richard H, Shivakant M. Defending against path based DoS attacks in wireless sensor networks. In the Proceedings of the 3rd Association for Computing Machinery (ACM) workshop on Security of ad hoc and sensor networks, Alexandria, Virginia, USA; 2005 Nov 5. p. 89–96.
8. Lindsey S, Raghavendra C. PEGASIS: Power Efficient Gathering in Sensor Information Systems. Institute of Electrical and Electronics Engineers (IEEE) Aerospace Conference Proceedings. 2002 Mar 9–16; 3:1125–30.
9. Subramanian G, Ramachandran A. Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. Journal of Communications and Networks. 2013 Aug; 15(4):422–9.
10. Supriya D, Ripul R. Review on LEACH-homogeneous and heterogeneous wireless sensor networks. International Journal of Innovative Research in Computer and Communication Engineering. 2015; 3(7):4442–7.
11. VanitaR, Dhir RR. A study of ad-hoc network: a review. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Mar; 3(3):135–8.
12. Chandirasekaran D, Jayabarathi T. A case study of bio-optimization techniques for wireless sensor network in node location awareness. Indian Journal of Science and Technology. 2015 Nov; 8(31):1–9. Crossref.
13. Devasena A, Sowmya B. Wireless sensor network in disaster management. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–6. Crossref.
14. Krishna KR, Rao KRRM. Hole detection and hole healing in a wireless sensor network using LeDiR methodology. Indian Journal of Science and Technology. 2016 Aug; 9(30):1–7. Crossref.
15. Asl VF, Vaziri B, Ravanmehr R. A method to detect data stream changes in the wireless sensor network using the gossiping protocol. Indian Journal of Science and Technology. 2016 Jul; 9(27):1–11.
16. Kothawade N, Biradar A, Kodmelwar K, Tambe KP, Deshpande V. Performance analysis of wireless sensor network by varying reporting rate. Indian Journal of Science and Technology. 2016 Jul; 9(26):1–6. Crossref.
17. Pathan ASK, Lee HW, Hong CS. Security in wireless sensor networks: issues and challenges. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 8th International Conference Advanced Communication Technology. 2006 Feb 20–22; 2:1048–54.
18. Chakrabarti S, Singhal M. Password-based authentication: preventing dictionary attacks. Institute of Electrical and Electronics Engineers (IEEE) Computer Society; 2007. p. 68–74.
19. Reddy MS, Rao KR. Fire accident detection and prevention monitoring system using wireless sensor network enabled android application. Indian Journal of Science and Technology. 2016 May; 9(17):1–5. Crossref.