IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 4 (Jul. - Aug. 2013), PP 101-111
www.iosrjournals.org

Energy Efficient and Secure, Trusted network discovery for Wireless Sensor Networks

Kumuda T P (M.Tech), Mrs. Sridevi K.N,
Department of computer science and engineering, CMR Institute of Technology, Bangalore, India.
Assoc. Professor Department of computer science and engineering, CMR Institute of Technology, Bangalore, India.

Abstract: *While routing Wireless Sensor nodes in the Multi-hop network ,nodes may undergo some attacks such as sink hole attack, worm hole attack, Sybil attack etc., by the attackers through identity deception. So, to secure WSN's against attackers or hackers misdirecting the nodes in the network while routing, in our base paper we have designed and implemented TARF, a robust trust aware routing framework concept for dynamic for WSN's. TARF provides trustworthy and energy-efficient route and also it provides security against all these attacks which are mentioned above. In our work, we are using modern technology like ECC i.e., Elliptic Curve Cryptography for encoding and decoding purpose. To know the performance of this TARF routing, in our paper we are comparing TARF Routing with Existing Routing and generating routing tables. To find the secure network discovery we are generating Combinatorial Key for Pre Key-Distribution in TARF Network. In the handheld devices like mobile we are trying to find the attacker information.*

Keywords: *Sinkhole attack, wormhole attack, Sybil attack, Elliptic Curve Cryptography, Pre Key-Distribution*

I. Introduction

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs were initially designed to facilitate military operations but its application has since been extended to health, traffic, and many other consumer and industrial areas. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multi-hop path.

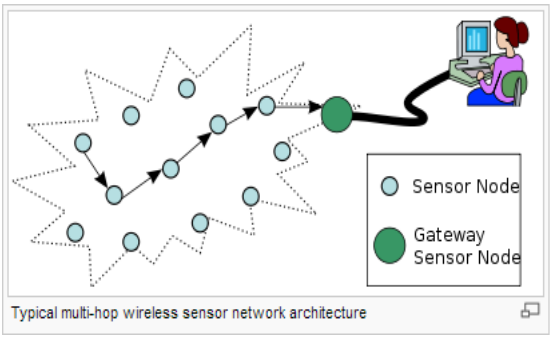

Fig-1 Typical multi-hop Wireless sensor network architecture

However multi-hop routing of wireless sensor nodes is the target for adversaries attacks. The attacker node can create the traffic collision with performing the valid transmission, they may tamper the nodes physically, they may jam the channel, they may drop or misdirect the data while routing. Based on the identity deception, the attacker node is able to perform some attacks on the nodes which are participating in multi-hop routing such as, selective routing, sink hole attack[6], worm hole attack[5], Sybil attack[4][7]. These networks have been subjected to numerous attacks among which Sinkhole attack is one of the notable ones.

In Sinkhole attack, sometimes the adversary node poses itself as a fake base station (BS) and receives all data of the network. It prevents data from reaching the main BS, or changes the received data and then transfers them to the main BS. In the Sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical Sinkhole with the adversary at the center. The harmful and easy-to –implement attack is wormhole attack, in which an attacker node simply replays all the data packets which are under the routing process from the valid node to gain the latter nodes identity so that next time he can use that forged identity to participate in the network easily. Soon after the attacker stealing the identity he can misdirect the network traffic such as, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed

among a few malicious nodes infinitely. Using same technique as in case of sinkhole attack we can have one more strong attack called Sybil attack.

The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility into WSNs and the hostile network condition. Though mobility is introduced into WSNs for efficient data collection and various applications [8], [9], [10], [11], it greatly increases the chance of interaction between the honest nodes and the attackers. Additionally, a poor network connection causes much difficulty in distinguishing between an attacker and a honest node with transient failure. Without proper protection, WSNs with existing routing protocols can be completely devastated under certain circumstances. In an emergent sensing application through WSNs, saving the network from being devastated becomes crucial to the success of the application.

As for as WSN's are concerned, secure routing solutions based on trust and reputation management rarely address the identity deception through replaying routing information. . At this point, to protect WSNs from the harmful attacks exploiting the replay of routing information, we have designed and implemented a robust trust-aware routing framework, TARF, to secure routing solutions in wireless sensor networks.

In our work, we are using modern technology like ECC [12] i.e., Elliptic Curve Cryptography for encoding and decoding purpose. To know the performance of this TARF routing, in our paper we are comparing TARF Routing with Existing Routing and generating routing tables. To find the secure network discovery we are generating Combinatorial Key for Pre Key-Distribution in TARF Network. In the handheld devices like mobile we are trying to find the attacker information.

II. Related papers

Wireless sensor networks (WSNs) [2] are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. We discuss more related work here in addition to the introduction in Section 1. It is generally hard to protect WSNs from *wormhole* attacks, *sinkhole* attacks and *Sybil* attacks based on identity deception.

In[1], To secure the WSNs against adversaries misdirecting the multi-hop routing, we have designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception.

In[3], This paper has presented an alternative method to confirm the trustworthiness of nodes in WSN. In this scheme involves designing a trusted platform and an energy efficient authentication protocol. The trusted mechanism has contributes to enhance security in WSNs by reducing the probability of fake or clone sensor node through non-regenerated unique platform identity.

In[12], In this paper we investigate what assumptions are necessary to gather information about the local network topology when adversarial nodes are present and capable of lying about their identity or neighbors in the network. combinatorial key pre-distribution scheme that allows a node to prove its identity by proving that it possesses just two keys from its key-list.

III. Problem statement

In Existing system, when the file send from base station in that situation hackers aggravated network conditions. A traditional cryptographic techniques effort does not address the severe problems. That time the file could be affected by hackers. So, the network will be damaged. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference.

Disadvantages:

1. There is no trusted authority to trust the nodes.
2. There is no Strong packet hiding methods for strong cryptography
3. No fixed routing instead Flooding in Routing will be there
4. No Attack Finders are there
5. Lack of less security due to DES and RSA Techniques

IV. Proposed system

TARF secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighboring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory *throughput*. TARF is also energy-efficient ,highly scalable, and well adaptable.

For an enhanced version of TARF routing system- enabled sender node to route a data packet to the destination node, sender node only needs to decide to which neighboring node it should forward the data packet

considering both the trustworthiness and energy efficiency. Once the data is forwarded to the next-hop node, the remaining job is to deliver the data packet to the destination node which is the responsibility of the intermediate nodes in the path, and the sender node is fully unaware of what routing decision its next-hop node makes. The sender node maintains a neighborhood table with trust level values and energy cost values for certain known neighbors. The technique of maintaining a neighborhood table of a moderate size is demonstrated by Woo, Tong and Culler [28]; TARF may employ the same technique.

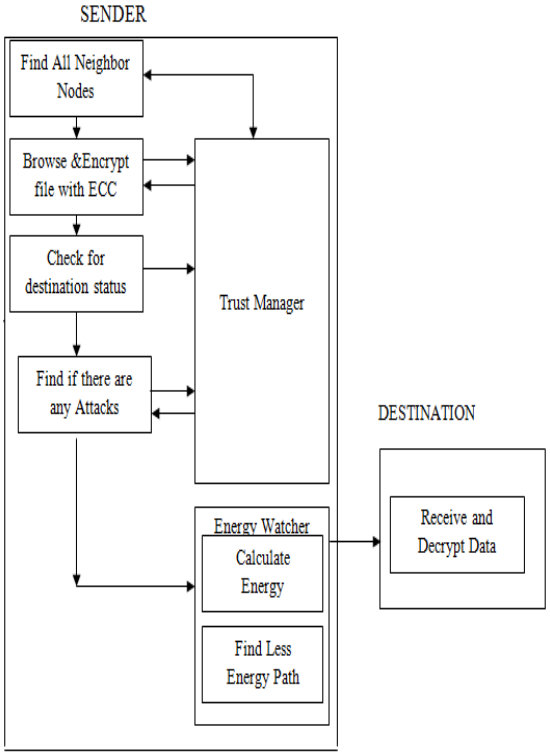

Fig 2: Architectural design of an enhanced TARF System.

Fig-2 shows the architectural design of our work. Initially sender node has to find all its neighboring nodes and based on the routing table the trust manager of the sender node will designs one trusted center. The trust manager of the sender node will be maintaining one trusted table for all the nodes, and it will be having one threshold value. That table contains every node's trusted value is more than that threshold value it will consider that node as un-trusted one otherwise it is trusted node . Next it will browse for the file to be send and encrypts using ECC algorithm then start all the nodes, which means that nodes will automatically fetch the certificate values from the trust manager and checks for the destination status whether that node is trusted one or not and checks whether any attacker is there in the path if it finds any intruder in between the path then it will select alternate path to send that packet. After its check if it finds that path is attacker free then only it will sends the packet through that path.

Next it the job of the energy watcher to calculate the total energy cost that packet has consumed to reach the destination. Disktra algorithm is used in this paper to find the less energy consuming path and Bellman ford algorithm to find the shortest path. For encryption ECC algorithm is used in this paper. Next section will discuss about this cryptographic algorithm.

4.1 Energy Watcher:

Energy cost is denoted as E, sender node as N and next-hop node as b. Here we describe how a sender node's *Energy-Watcher* computes the energy cost E_{Nb} for its neighbor b in N's neighborhood table and how N decides its own energy cost E_N. Before going further, we will clarify some notations. E_{Nb} mentioned is the average energy cost of successfully delivering a unit-sized data packet from N to the base station or destination node, with b as N's next-hop node being responsible for the remaining route. Here, one-hop re-transmission may occur until the acknowledgement is received or the number of re-transmissions reaches a certain threshold. The cost caused by one-hop retransmissions should be included when computing E_{Nb}.

Suppose N decides that A should be its next-hop node after comparing energy cost and trust level. Then N's energy cost is $E_N = E_{NA}$. Denote $E_{N!b}$ as the average energy cost of successfully delivering a data packet

from N to its neighbor b with one hop. Note that the retransmission cost needs to be considered. With the above notations, it is straightforward to establish the following relation:

$E_{Nb} = E_{N!b} + E_b$

4.2 Trust Manager:

A node N's *TrustManager* decides the trust level of each neighbor based on the following events: discovery of network loops, and broadcast from the base station about data delivery. For each neighbor b of N, T_{Nb} denotes the trust level of b in N's neighborhood table.

In the fig-3, node1has selected the path [1-2-4-7-10] initially, here node 10 has considered as a destination node or base station. The trust manager checks for the trust value of its neighboring node and checks for any attacks like sink hole or worm hole attack, if it finds any it will ask the sender node whether it can forward that packet through that route only or else it will asks to take an alternate path before sending the packet . in the fig 3 they is an attacker in the node 2 so it has taken alternate path as node[1-5-8-11-10]

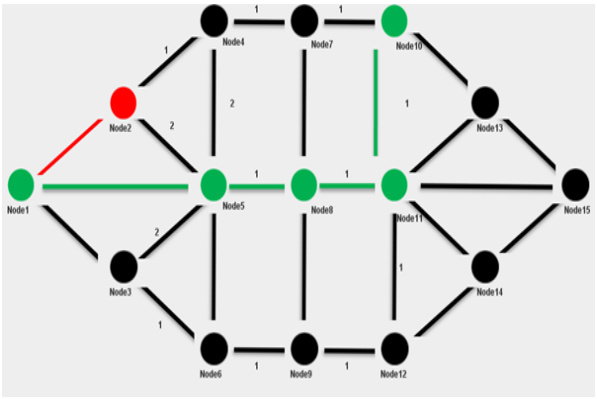

Fig.3.An example to illustrate how TrustManager works.

4.3 ECC Algorithm

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. Elliptic Curve Cryptography is one of the most interested research topic in VLSI. Network security is becoming more and more crucial as the volume of data being exchanged on the Internet increases.

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

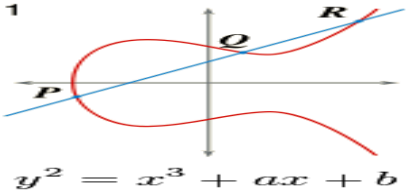

Fig-4, simple elliptic curve.

In this paper we are concentrating on this cryptographic technique. Here in this technique key generation is one of the important part, where we need to generate both public key and private key. The sender will be encrypting the message with receiver's public key and receiver will be decrypting using his own private key.

Now, we have to select a number **'d'** within the range of **'n'**.

Using the following equation we can generate the public key

Q = d*P

d = The random number that we have selected within the range of (**1 to n-1**). **P**is the point on the curve.

'Q' is the public key and **'d'** is the private key.

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

C1 = k * P

C2 = M + k * Q

C1 and C2 will be send.

Algorithm:

Input: Parameters field of elliptic curve (p,E,P,n), private key d, Plain text(C1, C2).

Output: Cipher text (C1,C2)

Begin

1. Represent the message m as a point M in E(Fp)
2. Select k Є g(1,n-1)
3. Compute C1 = kP
4. Compute C2 = M + kQ
5. Return (C1, C2)

End

Decryption

We have to get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that we have send.

Algorithm:

Input: Parameters field of elliptic curve (p,E,P,n), private key d, Cipher text(C1, C2).

Output: Plain text m

Begin

1. Compute M = C2 – dC1, and m from M.
2. Return (m)

End

Proof

How does we get back the message,

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1′

C2 – d * C1 = (M + k * Q) – d * (k * P)

(C2 = M + k * Q and C1 = k * P)= M + k * d * P – d * k *P (canceling out k * d * P)= M (Original Message)

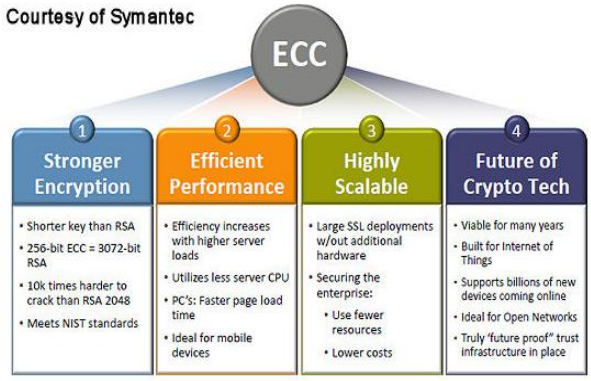

Fig 5: Advantages of using ECC cryptography algorithm

V. Simulation results

5.1 Network Certificate Generation:

Here Fig-6 shows Network Certificate Generation , before starting all the nodes in the network the trust manager will generates the certificate i.e.public key generation using RSA algorithm and signature using SHA256 with RSA algorithm.

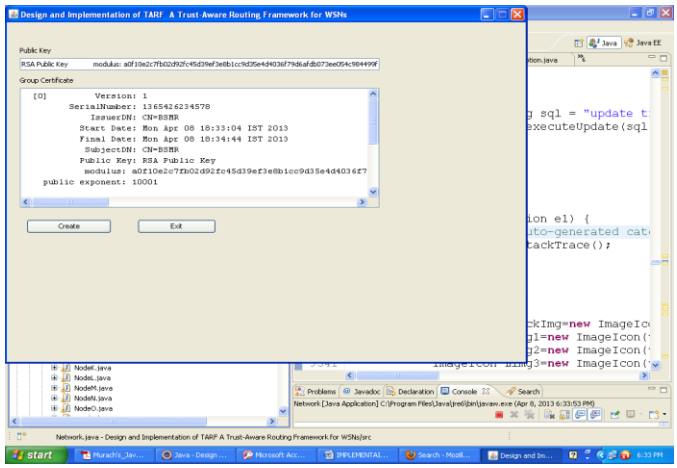

Fig-6 Network Certificate Generation

5.2 Nodes Interface

In Fig-7 we start all the nodes. Here all the nodes start generating the respective certificate to authenticate themselves to participate in the routing

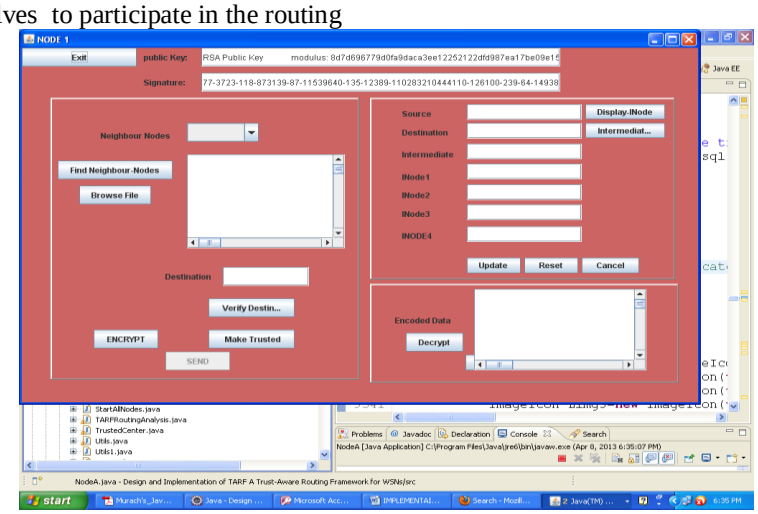

Fig-7 Nodes Interface

5.3 Trusted Center

The trust manager after starting all the nodes creates one Trusted Center based on the routing table. Here the Trust Manager initiates the trusted values for all the nodes in the Trusted Center.

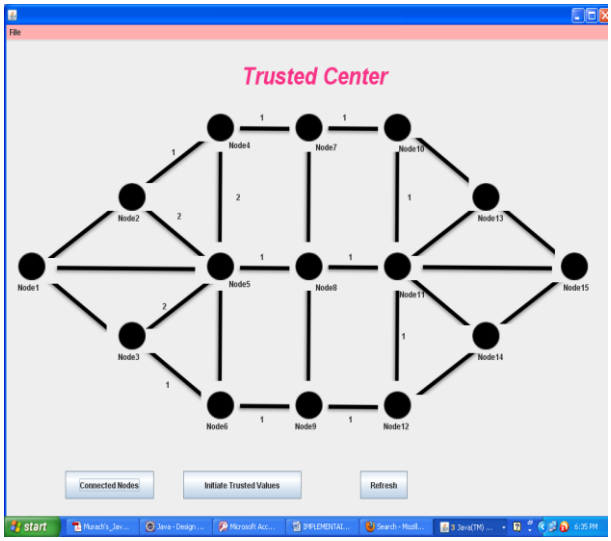

Fig-8 Trusted Center

5.4 Finding Neighboring Nodes:

In Fig-9(a) , Node 1 starts to find its neighboring nodes and then it selects through which path it can route the packet based upon the energy that packet consumes to reach its destination.

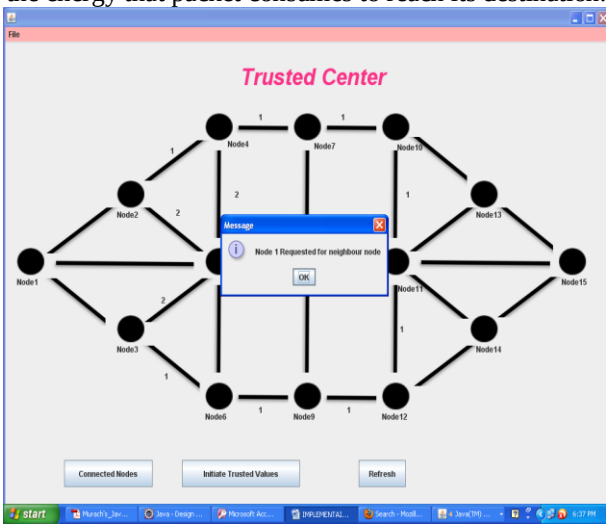

Fig-9(a) Node 1 Requesting for Neighbor Nodes

In Fig-9(b), shows node 1's neighboring nodes. According to that Trusted Center Architecture for node 1, nodes 2,3, and node 5. Among these three nodes node 1 selects only one path which consumes less energy to reach the destination node. Here in this example node 10 is the destination node.

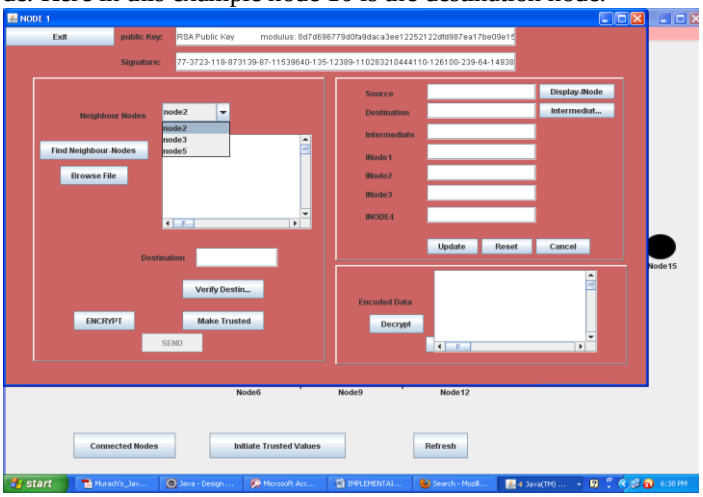

Fig-9(b) Node 1 Displays its Neighbor Nodes

5.5 Encryption using ECC algorithm

After finding its neighboring nodes here in this example the sender node i.e. node 1 has selected node 2 has its next-hop node since this is a shortest path and consumes less energy using dikstras and belmanford algorithm .Then browses the file to be send and encrypts using Elliptic curve cryptography.

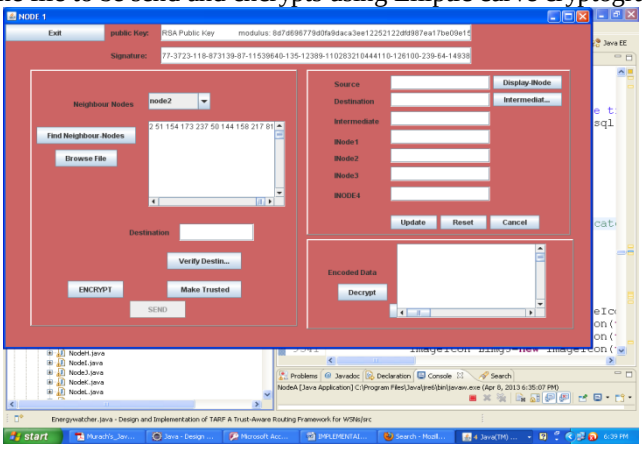

Fig-10 Browsing the file and encrypting the data using ECC algorithm

5.6 Check for Destination status

In this example node 10 is the destination node which is also a trusted node ,since its trusted value is less than threshold value .

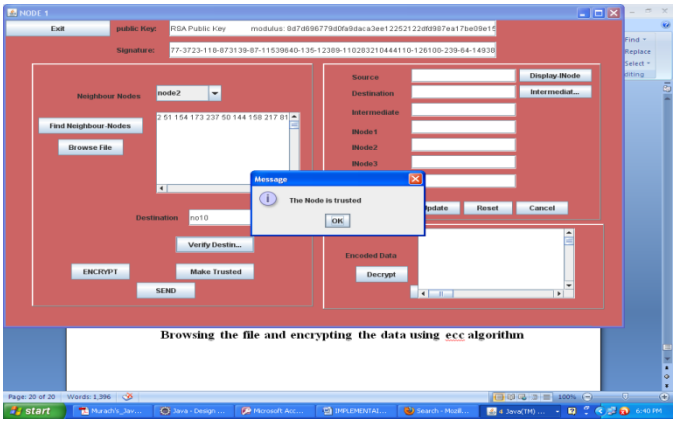

Fig-11, Checking the Destination node's trustworthiness

5.7 Successful Transmission

In fig-12(a), sender node has selected its next-hop node as node 2 i.e. the route will be through nodes[1,2,4,7,10] on successful transmission ,which means that ,in the path there are no attackers found.

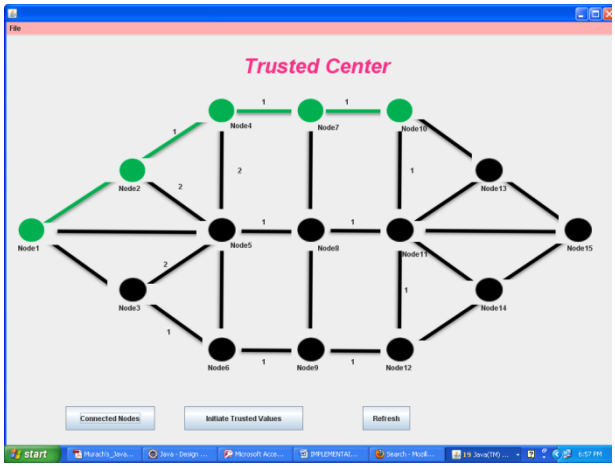

Fig-12(a) Successful transmission of the encrypted packet through the selected path

In Fig-12(b), The encrypted packet will reaches at the destination node or we can say that the packet reached at the base station.

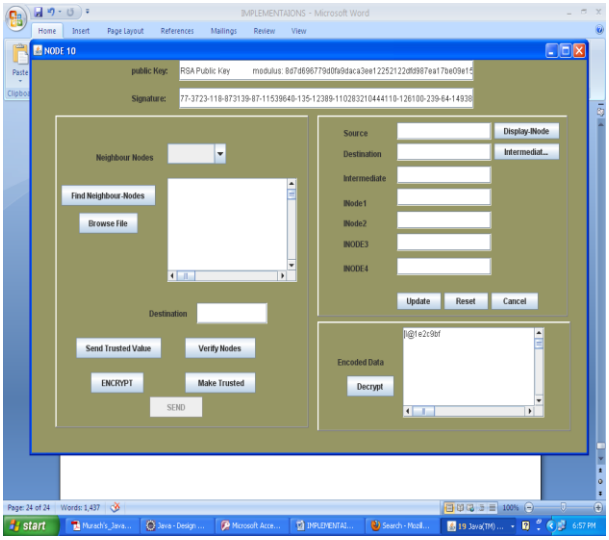

Fig-12(b) Encrypted data reception at the destination

In fig-12(c), the encrypted data has to decrypted by the destination node using the same cryptographic algorithm i.e. Elliptic Curve Cryptography.

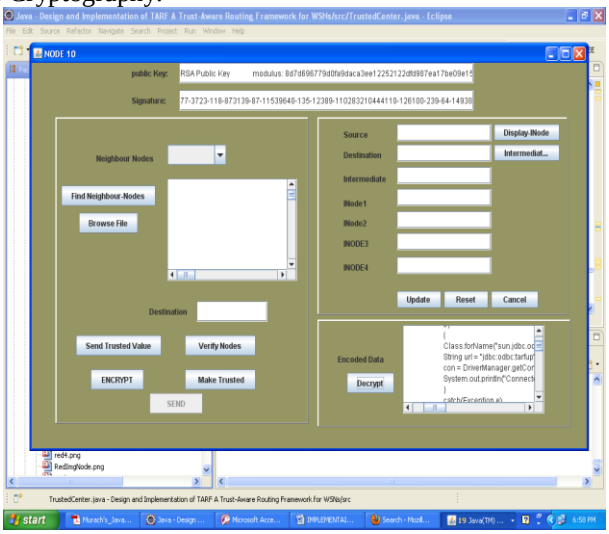

Fig-12© Decrypted data

5.8 Finding Attacks

In fig-13(a), before sending the packet only trust manager found that there is a Sinkhole attack in node 2. If the signature or the public keys of the nodes are different we can make out there is a sinkhole attack. Then it will ask for the sender whether it can choose for an alternative path or not. If the sender wish to proceed with the same path then packet will lost otherwise it can choose an alternative path.

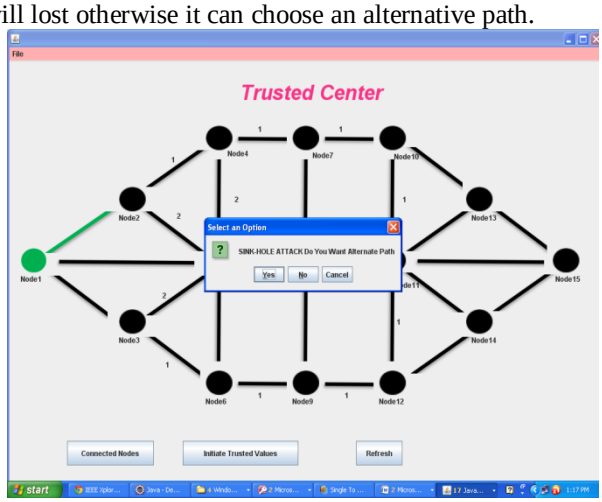

Fig-13(a),Sinkhole Attack

In fig-13(b), sender node as chosen an alternative path i.e through nodes[1,5,8,11,10]

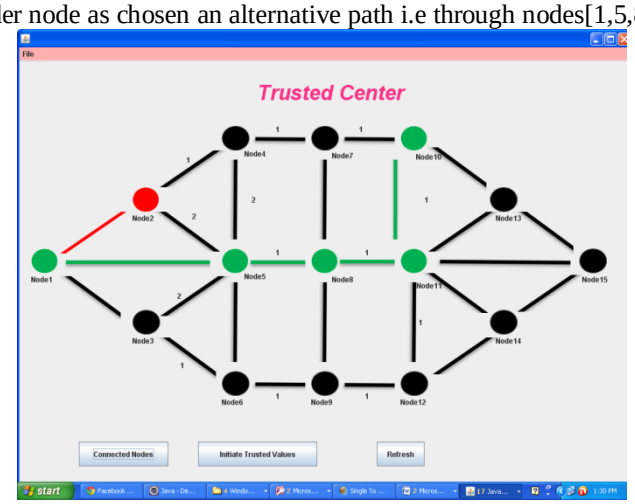

Fig-13(b), Alternate path

In fig-13©, they shown that there is an wormhole attack in the node 5 i.e. if there are any difference in the default routing table and the current routing table we can say that there is a wormhole attack. Here also it can choose for an alternative path.

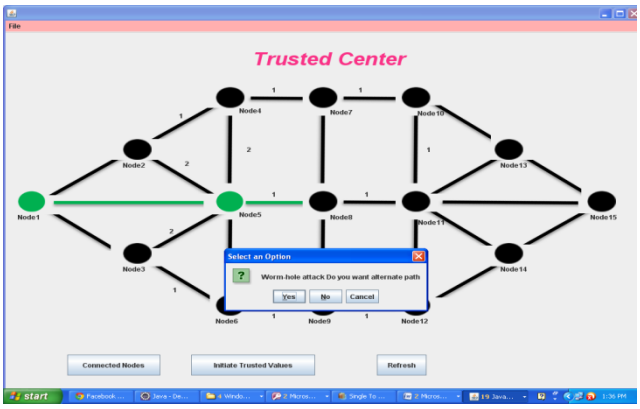

Fig-13©, Wormhole Attack

5.9 Energy Watcher

After the packet reaches the destination, energy watcher calculates the total energy cost.

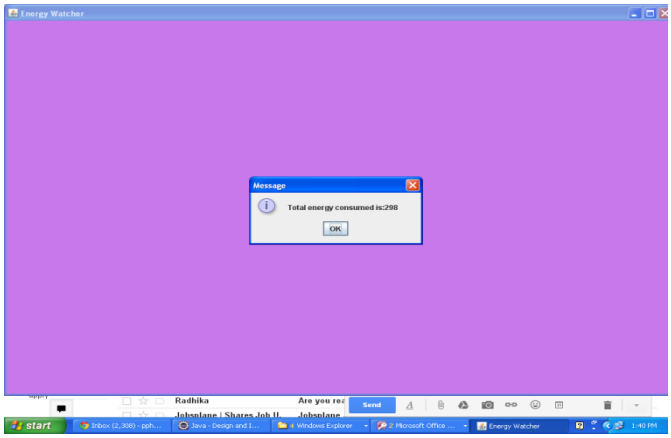

Fig-14, Energy watcher

In the paper we have shown the number of trusted and un-trusted nodes in the network. In the figure(15), it is shown that there are 10 trusted node and 5 un-trusted nodes in the network. This results are dynamically taken . Each time we initiate the nodes , each time the nodes will take different values . Based on those values it is calculating the number of trusted nodes and un-trusted nodes.

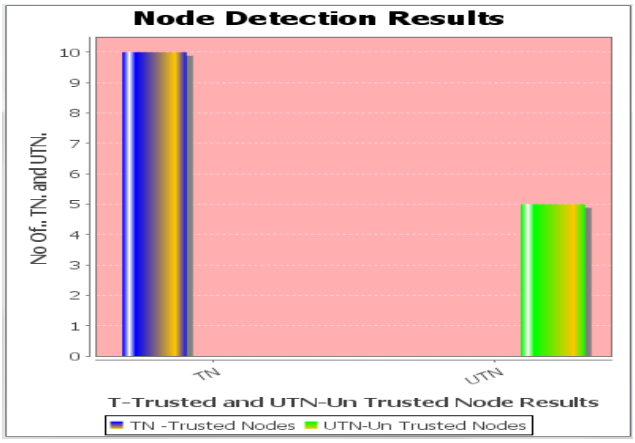

Fig-15 Trusted and untrusted node results

VI. Conclusion

We have designed and implemented a working model which is an enhanced version of TARF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information. TARF focuses on trustworthiness and energy efficiency. With the idea of trust management, our model enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. With the idea of the energy watcher, our model calculates the total energy cost which is consumed by the packet to reach its destination. Trust manager has introduced the concept of using two routing tables i.e default routing table and running routing table, with this concept its has become easy to find the attacker in the path. For providing security in this paper we have used the new encryption technique i.e. Elliptic Curve Cryptography algorithm.

Reference

[1] Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng, IEEE 2012 Transactions on Dependable and Secure Computing, Volume: 9 , Issue: 2:" Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs"

[2] F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann Publishers, 2004.

[3] Yusnani Mohd Yussoff1, Habibah Hashim2 and Mohd Dani Baba, IEEE Transaction on Dependable and Secure Computing,Vol 13,Issue 4: Identity-based Trusted Authentication in Wireless Sensor Network

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[5] M. Jain and H. Kandwal, "A survey on complex wormhole attack in wireless ad hoc networks," in Proceedings of International Conference on Advances in Computing, Control, and Telecommunication Technologies (ACT '09), 28-29 2009, pp. 555 –558.

[6] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WIMOB '08), 12-14 2008, pp. 526 –531.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," in Proc. of the 3rd International Conference on Information Processing in Sensor Networks (IPSN'04), Apr. 2004.

[8] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance analysis of mobile agent-based wireless sensor network," in Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009), 20-24 2009, pp. 16 –19.

[9] L. Zhang, Q. Wang, and X. Shu, "A mobile-agent-based middleware for wireless sensor networks data fusion," in Proceedings of Instrumentation and Measurement Technology Conference (I2MTC '09), 5-7 2009, pp. 378 –383.

[10] W. Xue, J. Aiguo, and W. Sheng, "Mobile agent based moving target methods in wireless sensor networks," in IEEE International Symposium on Communications and Information Technology (ISCIT 2005), vol. 1, 12-14 2005, pp. 22 – 26.

[11] J. Hee-Jin, N. Choon-Sung, J. Yi-Seok, and S. Dong-Ryeol, "A mobile agent based leach in wireless sensor networks," in Proceedings of the 10th International Conference on Advanced Communication Technology (ICACT 2008), vol. 1, 17-20 2008, pp. 75 –78.

[12] International Journal of Computer Applications (0975 – 8887) Volume 8– No.3, October 2010 "High Speed and Low Space Complexity FPGA Based ECC Processor".

[13] Kevin Henry, Douglas R. Stinson, IEEE On Lightweight Security & Privacy: Devices, Protocols and Applications,VOL:21,14-15 March 2011 " Secure Network Discovery in Wireless Sensor Networks Using Combinatorial Key Pre-Distribution"