e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

Trusted Routing Path Selection in WSNs through TARF

[1]M.P.Vijaya Kumar, [2]Dr. Monica R Mundada

[1]*Asst. Professor, Department of CSE, MMCT, Mangalore, India*

[2]*Associate Professor, Department of CSE, MSRIT, Bangalore, India*

Abstract-In wireless Sensor Networks data transfer is insecure, because the intruders may use duplicate IP address to hack the confidential data. Hop by hop authentication is necessary for secured communication to prevent such confidentiality Multi hop routing in Wireless sensor networks (WSNs) offers little protection against the identity deception through replaying routing information. This defect may take a chance of an adversary to misdirect significant network traffic, resulting in disastrous consequences attacks against the routing protocols including Sinkhole, Worm hole and Sybil attacks. The situation is further aggravated by mobile & harsh network condition. It cannot be solved by traditional encryption or authentication techniques or efforts at developing trust aware routing protocols do not effectively address this severe problem. Secure the WSNs against adversaries misdirecting the multi-hop routing. So proposed a method is "Trusted Routing Path Selection in WSNs through TARF", a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information. TARF provides trustworthy, secure, time efficient & energy efficient route. Most importantly TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large scale WSNs under various scenarios.

Keywords-Trust Manger, Trusted node, Un-trusted node, WSNs (Wireless Sensor Networks), ECC (Elliptic Curve Cryptography), Sinkhole Attack, Wormhole Attack, Sybil Attack.

I. INTRODUCTION

However the multi–hop routing of WSNs often becomes the target of malicious attacks. 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. This thesis highlighted such kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception, the adversary is capable of launching harmful & hard to detect attacks against routing. Such as selective forwarding, wormhole attacks, sinkhole attacks & Sybil attacks.

As a harmful & easy to implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity; the malicious node then uses this forged identity to participate in the network routing, thus disrupting the network traffic. Those routing packets, including their original headers are replayed without any modification. Even if this malicious node can't directly overhear the valid node's wireless transmission, it can collude with other malicious nodes to receive those routing packets & replay them somewhere far away from the original valid node, which is known as a wormhole attack.

Since a node in a WSN usually relies solely on the packets received to know about the sender's identity, replaying routing packets allows the malicious node to forge the identity of this valid node. After "stealing" that valid identity, this malicious node is able to misdirect the network traffic. For instance, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even from a transmission loop through which packets are passed among a few malicious node infinitely. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques.

Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a “block hole”. This same technique can be employed to conduct another strong form of attack-Sybil attack: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks. A poor network connection causes much difficulty in distinguishing between an attacker & 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. Unfortunately, most existing routing protocols for WSNs both assume the honesty of nodes & focus on energy efficiency, or attempt to exclude unauthorized participation by encrypting data & authenticating packets. Examples of these encryption and authentication schemes for WSNs include Tiny Sec, Tiny PK, and Tiny ECC. Admittedly, it is important to consider efficient energy for battery powered sensors nodes and the robustness of routing under topological changes as well as common faults in a wild environment. However, it is also critical to incorporate security as one of the most important goals; meanwhile, even with perfect encryption and authentication, by replaying routing information, a malicious node can still participate in the network using another valid node’s identity.

It is important to consider efficient energy use or battery powered sensor nodes & the robustness of routing under topological changes as well as common faults in a wild environment. However, it is also critical to incorporate security as one of the most important goals; meanwhile, even with perfect encryption & authentication, by replaying routing information, a malicious node can still participate in the network using another valid node’s identity. The gossiping based routing protocols offers certain protection against attackers by selecting random neighbors to forward packets, but at a price of consideration overhead in propagation time & energy use. In addition to the cryptographic methods, trust & reputation management has been employed in generic ad hoc network & WSNs to secure routing protocols, basically a system of trust value according to its past performance in routing. Then such trust values are used to help decide a secure & efficient route.

However, the proposed trust & reputation management systems for generic ad hoc networks target only relatively powerful Hardware platform such as laptops & smart phones. Those systems can not be applied to WSNs due to the excessive overhead for resource constrained sensor nodes powered by batteries.

As far as WSNs are concerned, secure routing solutions based on trust & reputation management rarely address the identity deception through replaying routing information. The countermeasures proposed so far strongly depends on either tight time synchronization or known geographic information while their effectiveness against attacks exploiting the replay of routing information has not been examined yet. At this point, to protect WSNs from the harmful attacks exploiting the replay of routing information, we have designed & implemented a robust trust-aware routing framework, TARF to secure routing solution in WSNs. Based on the unique characteristics of resource-constrained WSNs, the design of TARF centers on trustworthiness & energy efficiency. Through TARF can be developed into a complete & independent routing protocol , the purpose is to allow existing routing protocols to incorporate our implementation of TARF with the least effort & thus producing a secure & efficient fully-functional protocol. Unlike other security measures, TARF requires neither tight time synchronization nor known geographic information.

Most importantly, TARF proves resilient under various attacks exploiting the replay of routing information, which is not achieved by previous security protocols. Even under strong attacks such as sinkhole attacks, wormhole attacks as well as Sybil attacks, and hostile mobile network condition. TARF demonstrate steady improvement in network performance. The effectiveness of TARF is verified through extensive evaluation with simulation & empirical experiments on large-scale WSNs.

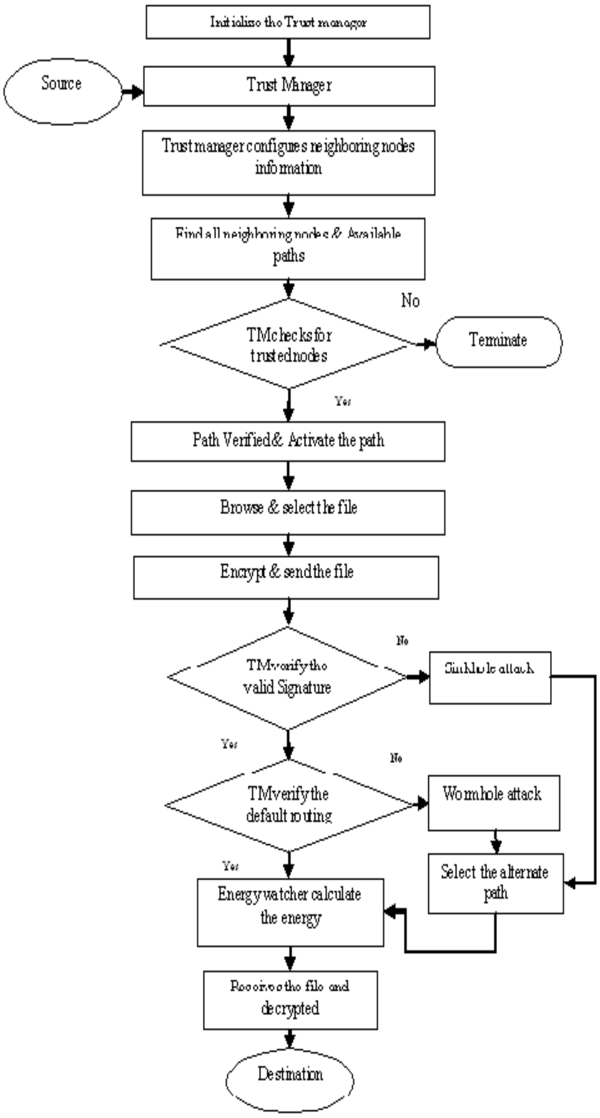
II. GOALS

- **Routing the network:** In this module, the networks embedded on the physical fiber topology. However, assessing the performance reliability achieved independent logical links can share the same physical link, which can lead to correlated failures. Mainly, we focus on assessing the reliability of energy level and trusted network.
- **High Throughput:** Throughput is defined as the ratio of the number of all data packets delivered to the base station to be number of all sampled data packet. Though put reflects how efficiently the network is collecting and delivering data.
- **Energy Efficiency:** Data transmission accounts for a major portion of the energy consumption. We evaluate energy efficiency by the average cost of successfully deliver a unit-sized data packets from node to the base station. Be given enough attention when considering energy cost since each retransmission causes a noticeable increase in energy consumption. If every node in a WSN consumes approximately the same energy to transmit a unit-sized data packet, we can use another metric hop-delivery to evaluate energy efficiency. Under that assumption, the energy consumption depends on the number of hops, i.e. the number of one-hop transmission occurring. To evaluate how efficiently energy is used, we can measure the average hops that each delivery of a data packet takes, abbreviated as hop-per-delivery.
- **Transfer file:** In this module, analysis the shortest path algorithm independently routes each logical link on a physical path with the minimum number of hops in trusted basis. Since we are assuming that every physical links fail with the same probability, the failure probability of path is minimized when it is routed over the shortest path, each light-path greedily takes the most reliable route and transfer the file.
- **Sink hole and Wormhole attacks:**

- Prevent the base station from obtaining complete and correct sensing data
- Some secure or geographic based routing protocols resist to the sinkhole attacks in certain level
- Many current routing continuously monitor their surroundings forward the sensing data to a sink node or base station
- Particularly severe for wireless sensor networks
- Many-to-one Communication vulnerable to the sinkhole attack, where an intruder attacks surrounding nodes with Unfaithful routing information alters the data passing through it or performs selective forwarding.

- **Energy Watcher and Trust manager:** In this module Cluster based WSNs allows for great savings of energy and bandwidth through aggregation data from children nodes and performing routing and transmission for children nodes. In a cluster based WSN, the cluster headers themselves form a sub-networks, after certain data reach a cluster header, the aggregated data will be routed to a base station only through such a sub network consisting of the cluster header. Our framework can then be applied to this sub-network to achieve secure routing for cluster based WSNs. Trust Manager encourages a node to choose another route when it's current frequently fails to deliver data to the base station. Though only those legal neighboring nodes of an attacker might have correctly identified the adversary

III. PROPOSED METHODLOGY


Initialise the Trust manager
Source
Trust Manager
Trust manager configures neighboring nodes information
Find all neighboring nodes & Available paths
TM checks for trusted nodes
No
Terminate
Yes
Path Verified & Activate the path
Browse & select the file
Encrypt & send the file
TM verify the valid Signature
No
Sinkhole attack
Yes
TM verify the default routing
No
Wormhole attack
Select the alternate path
Yes
Energy watcher calculate the energy
Receive the file and decrypted
Destination

3.1 Overall Proposed System Architecture

As shown in above figure is the overall system architecture. Figure 3.2(a) and Figure 3.2(b) represents initial state. When source node send request to the trust manager (Figure 3.2(c), (d), (e), (f)) trust manager will be first check the neighbor nodes and destination node. If the destination node is trusted or un-trusted depending upon the previous successive data transfer and participates in that networks, depending on this trust manager will consider the node energy and assign the trust value of the nodes. If the destination node is trusted then only trust manager assign send button in source node (Figure 3.2(f)) otherwise disabled in source node. After send button enabled source node will select the file and encrypted using ECC method (Figure 3.2(e), (f)) send the file. After send the file, trust manager check the shortest path, check the valid signature and default routing table. In intermediate nodes valid identity (here we called signature) assign by trust manager & is verify the valid identity.

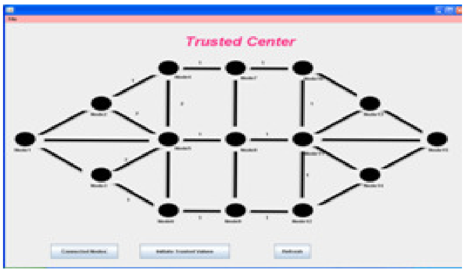
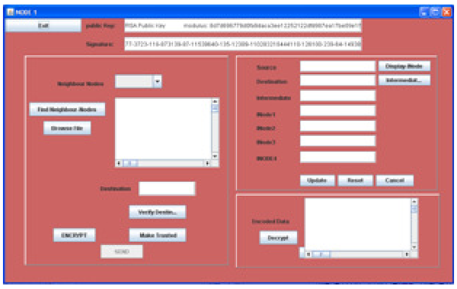


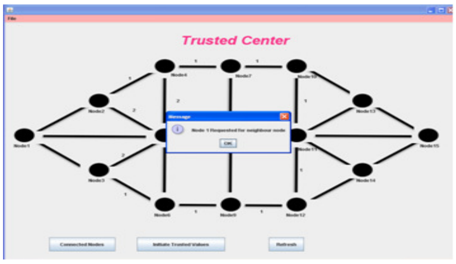
Figure 3.2(a)



public Key: RSA Public Key modulus: 8d7d696779d0fa9daca3ee12252122dfd987ea17be09e15

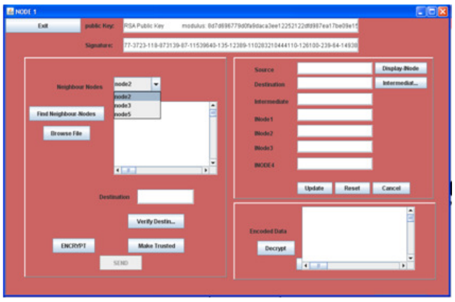
Signature: 77-3723-118-873139-87-11539640-135-12389-110283210444110-126100-239-64-14938

Figure 3.2(b)



Node 1 Requested for neighbour node

Figure 3.2(c)

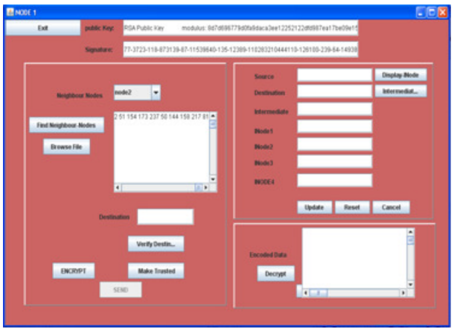


public Key: RSA Public Key modulus: 8d7d696779d0fa9daca3ee12252122dfd987ea17be09e15

Signature: 77-3723-118-873139-87-11539640-135-12389-110283210444110-126100-239-64-14938

Neighbour Nodes: node2
node2
node3
node5

Figure 3.2(d)



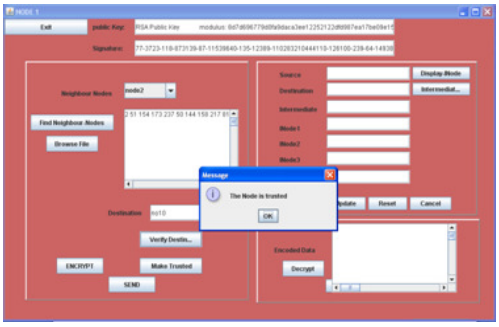
public Key: RSA Public Key modulus: 8d7d696779d0fa9daca3ee12252122dfd987ea17be09e15

Signature: 77-3723-118-873139-87-11539640-135-12389-110283210444110-126100-239-64-14938

Neighbour Nodes: node2

2 51 154 173 237 50 144 158 217 81

Figure 3.2(e)



public Key: RSA Public Key modulus: 8d7d696779d0fa9daca3ee12252122dfd987ea17be09e15

Signature: 77-3723-118-873139-87-11539640-135-12389-110283210444110-126100-239-64-14938

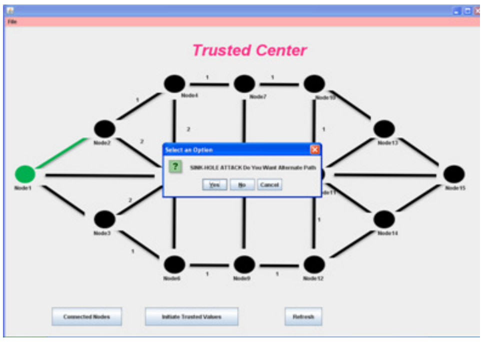
Neighbour Nodes: node2

2 51 154 173 237 50 144 158 217 81

Destination: node10

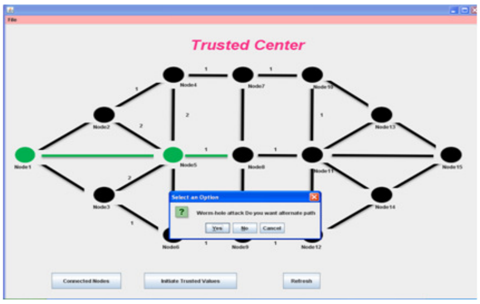
The Node is trusted

Figure 3.2(f)



SINK-HOLE ATTACK Do You Want Alternate Path

Figure 3.2(g)



Worm-hole attack Do you want alternate path

Figure 3.2(h)

When source node send the file to destination through intermediate nodes, then trust manager will identify the valid signature, if any alter or change the identity by hacker trust manager will identify as sinkhole attack (Figure 3.2(g)) and then trust manager selecting the alternate path from that hacked node to the destination node (Figure 3.2(i)). Trust manager also check the default routing table and node routing table. If its any alter in routing tale trust manager will identify as wormhole attack (Figure 3.2(h)) and select alternate path (Figure 3.2(j)). Finally destination node receives that file decrypted by using their private keys. Energy watcher will responsible for updating the nodes energy. Through TARF selecting the trusted routing path in WSNs is very useful and efficient because hackers may hack the important data and some time intermediate node are not efficient energy so trust manager will identify these disadvantages and selecting trusted routing path in WSNs through TARF.

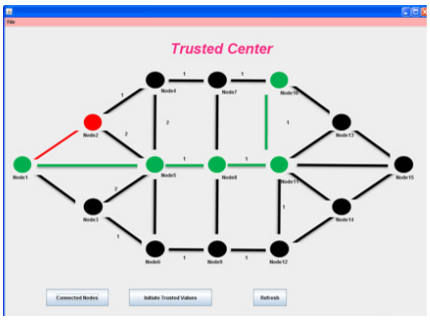


Figure 3.2(i)

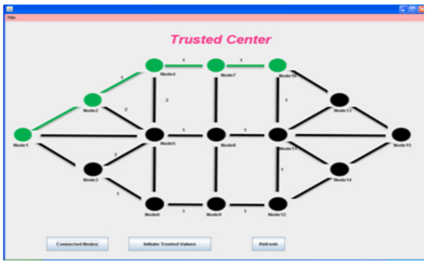
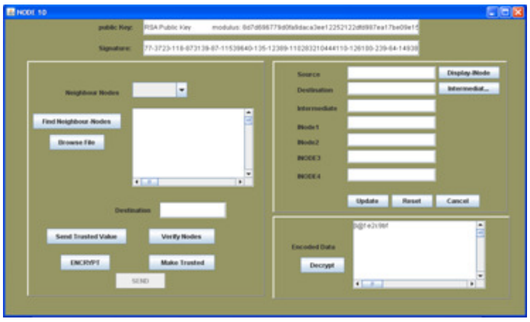


Figure 3.2(j)

Figure 3.2(k) shows encrypted data in bits format in receiver side and Figure 3.2(l) shows receiver receives the encrypted bits file and decrypted that file safely using ECC method.

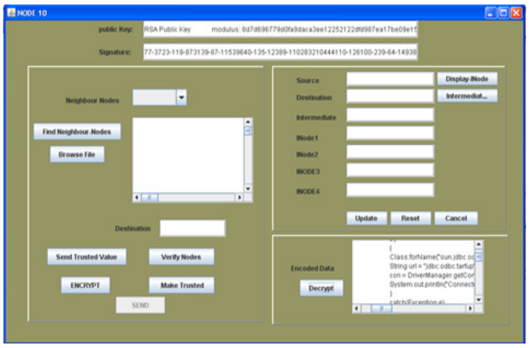


public Key: RSA Public Key modulus: 8d7d696779d0fa9daca3ee12252122dfd987ea17be09e15

Signature: 77-3723-118-873139-87-11539640-135-12389-110283210444110-126100-239-64-14938

Encoded Data: b@f+e2c9bf

Figure 3.2(k)



public Key: RSA Public Key modulus: 8d7d696779d0fa9daca3ee12252122dfd987ea17be09e15

Signature: 77-3723-118-873139-87-11539640-135-12389-110283210444110-126100-239-64-14938

Encoded Data:

```
{
Class.forName("sun.jdbc.od
String url = "jdbc:odbc:tarfup"
con = DriverManager.getCon
System.out.println("Connect
}
catch(Exception e)
```

Figure 3.2(l)

IV. CONCLUSION AND FUTURE ENHANCEMENT

We have designed and implemented 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, which are vital to the survival of WSNs in a hostile environment. With the idea of trust management, TARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. Unlike previous effort at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information: it requires neither tight time Synchronization nor known geographic information. The resilience and scalability of TARF is proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves static and mobile setting, hostile network conditions, as well as strong attack such as sinkhole, wormhole and Sybil attack.

Likewise the data to be secured in wireless sensor network system. This is verified with the very few nodes: this can be implemented with many numbers of nodes. The system has much scope in the future and it can be developed to add more features.

REFERENCES

[1]. Yanli Yu, Keqiu Li, Wanlei Zhou, Ping Li, "Trust mechanism in wireless networks: Attacks analysis and counter measures", journal of Networks and Computer Applications 35 (2012), Page 867-880.

[2]. Randhir Kumar, Akash Anil, "Implementation of Elliptic Curve cryptography",IJCSI International Journal of Computer Science Issues, Vol 8, Issue 4, No 2, July 2011.

[3]. F. Amounas and E.H Ei Kinani, "ECC Encryption and Decryption with a Data Sequence", Mathematical sciences, Vol 6, 2012, no. 101, 5039-5047

[4]. Ansgar Kellner, Kerstin Behrends, Dieter Hogrefe,"Challenges of Secure Routing in WSNs: a Survey", Georg-August-universitat Gottingen Institute of Computer Science, ISSN 1611-1044