INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

***ISSN: 2278 – 0211 (Online)***

# Development Of An Efficient Secured Multi-Hop Routing Technique For Wireless Sensor Networks

**Rijin I.K**
II Year M.E (CSE), VSB Engineering College, India
**Dr.N.K.Sakthivel**
Professor /CSE, VSB Engineering College, India
**Dr.S.Subasree**
[3=]Professor/IT, VSB Engineering College, India

***Abstract:***

*Wireless Sensor Networks utilize large numbers of Wireless Sensor nodes to forward information from source to destination. Wireless Sensor Nodes are battery-powered devices. Energy saving is always vital to maximize the lifetime of Wireless Sensor Networks. Recently, there are many Routing Protocols have been designed and proposed for Wireless Sensor Networks to improve its performance in terms of Communication Time, Residual Energy and Energy Consumption. An Efficient HYbrid Multi-hop routiNg (HYMN) Technique was proposed recently, which was a hybrid of the two contemporary Multi-Hop Routing Techniques, namely, Flat Multi- Hop Routing Technique and Hierarchical Multi-Hop Routing Technique. It demonstrates the effective performance in terms of Network Lifetime and superior connectivity. However, from the literature survey, it is observed that this Hybrid Multi-Hop Routing Technique fails to achieve sinkhole attacks, which are the major noted attacks against this Hybrid Multi-Hop Routing Technique. To address this issue and to secure the Wireless Sensor Networks against the above mentioned attacks, this research work is planned to enhance the Hybrid Multi-Hop Routing Technique with Trust-Aware Routing Framework, which will improve the performance of Wireless Sensor Networks in terms of trustworthy and Network Lifetime.*

***Key words:*** *Wireless sensor networks, routing protocols, security.*

**1.Introduction**

A wireless sensor network consists of a possibly large number of wireless devices able to take environmental measurements. Typical examples include temperature, light, sound, and humidity. These sensor readings are transmitted over a wireless channel to a running application that makes decisions based on these sensor readings. A WSN comprises battery-powered sensor nodes with extremely limited processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multihop path. However, the multihop 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

In this paper, an Efficient Secured Multi-Hop Routing Technique is proposed. our proposal is focuses on the kind of attacks in Hybrid Multi-hop routiNg (HYMN)[1]which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception [2], the adversary is capable of launching harmful and hard-to detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks and Sybil attacks [2,3].

**2.Related Work**

In WSNs, data gathering using multi-hop transmissions usually causes a problem to the sensor nodes which are close to the BS that, because of acting as intermediaries for data transmission, their energy would exhaust faster. It is called self-induced black hole problem or energy hole problem[6], To address this issue and to make an energy efficient routing mechanisms Ahmed E.A.A. Abdulla, et al presented A Novel Hybrid Multi-Hop Routing Algorithm to Improve the Longevity of WSNs(HYMN),Heinzelman, et al. presented the LEACH (Low- Energy Adaptive Clustering Hierarchy) protocol for WSNs of cluster-based architecture[4], which is a widely known and elegant clustering algorithm, by selecting the CHs in rounds. LEACH achieved improvement compared to direct transmissions, as measured in terms of nodes' lifetime, In this paper, for convenience, we call this kind of routing algorithms.

The multihop routing in wireless sensor networks offers little protection against identity deception through replaying routing information[7]. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks and Sybil attacks[3,5]. To address this issue Guoxing Zhan,et

al. proposed A Trust-Aware Routing Framework[2] for WSNs Following the idea of TARF algorithm, a number of algorithms have been presented in this work it use these kinds of frame works for providing security in the WSNs system

**3.Proposed Efficient Secured Multi-Hop Routing Technique For Wireless Sensor Network (ES-MHRT)**

This research work is planned to enhance the Hybrid Multi-Hop Routing Technique with Trust-Aware Routing Framework, which will improve the performance of Wireless Sensor Networks in terms of trustworthy and Network Lifetime.

*3.1.Architecture For ES-MHRT*

ES-MHRT secures the hybrid multi hop routing in WSNs against intruders misdirecting the hybrid multi hop routing by evaluating the trustworthiness of neighbouring nodes(Fig.1). Before introducing the detailed design, we first introduce several necessary notions here.

- Neighbour: For a node N, a neighbour (neighbouring node) of N is a node that is reachable from N with one-hop wireless transmission.
- Trust level: For a node N, the trust level of a neighbour is a decimal number in [0, 1], representing N's opinion of that neighbour's level of trustworthiness. Specifically, the trust Level of the neighbour is N's estimation of the probability that this neighbour correctly delivers data received to the base station.

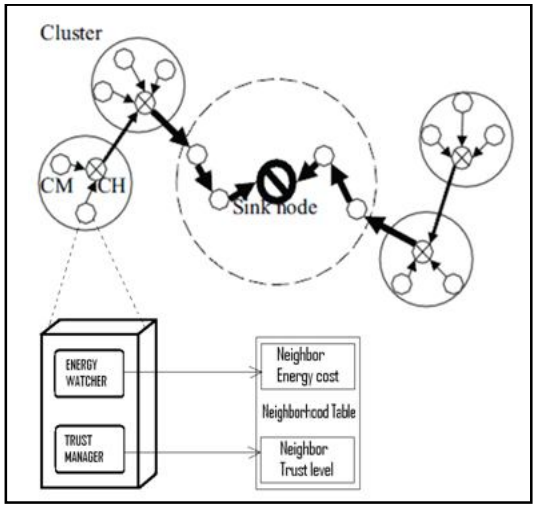


*Figure 1: Architecture of ES-MHRT*

- Energy cost: For a node N, the energy cost of a neighbour is the average energy cost to successfully deliver a unit sized data packet with this neighbour as its next-hop node, from N to the base station.
- Energy Watcher: it is responsible for recording the energy cost for each known neighbour, based on N's observation of one hop transmission to reach its neighbours and the energy cost report from those neighbours.
- Trust Manager: it is responsible for tracking trust level values of neighbours based on network loop discovery and broadcast messages from the base station about data delivery.

## 4. PROPOSED TECHNIQUES

The following techniques are used to improve the trust and network life time of WSNs in ES-MHRT.

### *4.1.Energy Cost Management*

For finding the energy cost of the node it uses the following equation

$$E_{nb} = E_{n->b} + E_b$$

Where

$E_{nb}$ ---> Energy cost of node b

$E_{n->b}$ --->Energy required sending a packet from node n to node b

$E_b$ ---> Energy level of node

### *4.2.Trust Management*

The implementation of this new protocol decides the next-hop neighbour for a node with two steps : Step 1traverses the neighbourhood table for an optimal candidate for the next hop; Step 2 decides whether to switch from the current next-hop node to the optimal candidate found.

//the cost of routing via the optimal candidate provided by the existing protocol, initially infinity

Optimal_cost=MAX_COST

//the trust level of the optimal candidate, initially 0

Optimal _trust=MIN_TRUST

For each candidate in the neighbourhood table

```
If  link is congested, or may cause a loop ,or does not  pass quality threshold
        continue
better=false
If candidate.trust >= optimal_trust  && candidate.cost<optimal_cost
        better=true
//prefer trustworthy candidates
If candidate.trust >=TRUST_THRESHOLD&& optimal_trust<TRUST_THRESHOLD
        better=true
//effective when all nodes have low trust due to network change or poor connectivity
If candidate.trust>=3*optimal_trust/2
        better=true
//add restriction of trust level requirement
If candidate.trust>=TRUST_THRESHOLD&&candidate.trust/candidate.cost> optimal_trust/optimal_cost
        better=true
If better ==true
        Optimal_candidate=candidate
        Optimal_cost=candidate.cost
        Optimal_trust=candidate.trust
//step 2. Decide whether to switch from the current next-hop to the optimal candidate
If optimal_trust>=currentNextHop.trust||currentNextHop.trust<=TRUST_THRESHOLD||current link is congested and switching is not likely to cause loops
```

**5.Implementation And Results**

We used a reconfigurable emulator for this work The maximum sensor node capacity for the network is 50 and each nod in the WSN will launch as a separate window user can manually change the operational states of the node or system will automatically set the different operational state, and the battery power and trust level of all the nodes initially equal to 100%.There are mainly six operational states are there in a wireless sensor networks which are active, transive, idle, transmit, receive and sleep .

The execution consists of two stages deploying the network and running the tool. After deploying the network, the properties of the network should be set using the network properties buttons. The network configuration properties will set automatically.

| | |
|---|---|
| Number of nodes | 9 |
| Transmitter node | Node 0 |
| Receiver node | Node 4 |
| Encryption algorithm | RAC |
| Data Size | 14186 B |

*Table 1: Experimental data*

When the network parameters are set, the network can be deployed Once the network has been deployed, run the hack tool & motes emulator then select the source and destination folder for the file to be transmitted(use encryption and decryption button for providing security for the data)

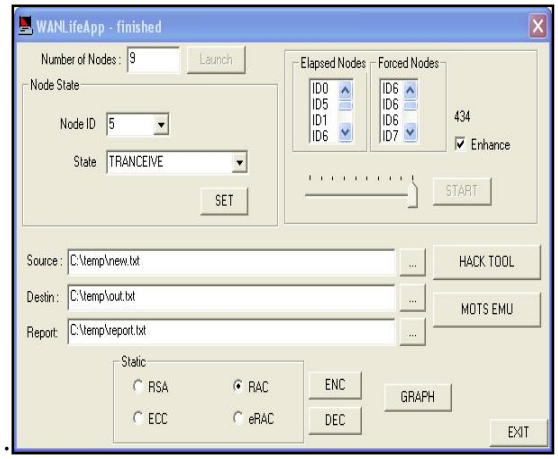


*Figure 2: Final window*

The sensors may run out of power and drop out of the network, and eventually, all nodes will be powered down. The progress of the network can be monitored via the elapsed nodes and forced nodes box (Fig.2).

*5.1.Network Lifetime*

The lifetime of a sensor network is most commonly defined as the time to the first sensor node failure It has been shown(Fig.3) that network lifetime of ES-MHRT network is increasing (63H) compared to HYMN(49H).

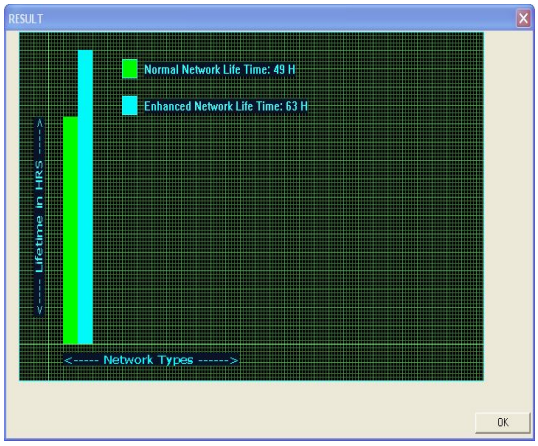


*Figure 3: Network Lifetime*

*5.2.Security Level*

Security is an essential feature for ES-MHRT. The ES-MHRT should be able to handle both wormhole attack and sink whole attack It has been shown that(Fig.4) the total Security level in a ES-MHRT network is increased (84%) compared to HYMN network(74%).

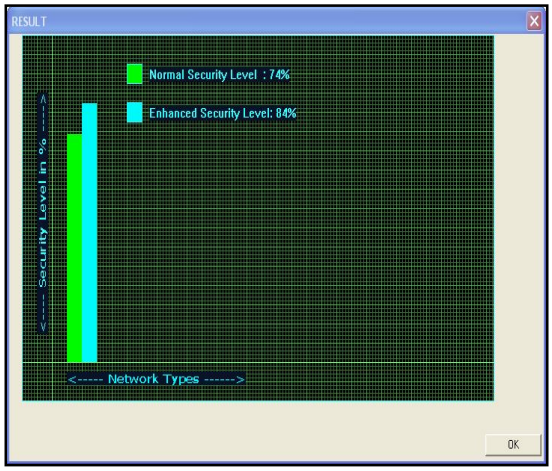


*Figure 4: Security Level*

*5.3.Energy Consumption*

Saving energy is a very critical issue in wireless sensor networks (WSNs), In this work, it has been shown that (Fig.5) the total energy consumption in a ES-MHRT network is reduced (5W) compared to HYMN(9W).

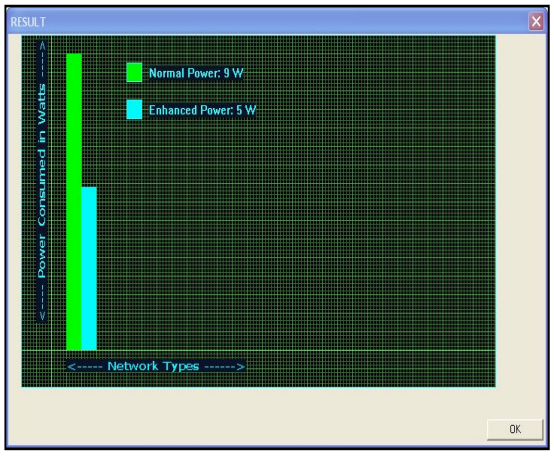


*Figure 5: Energy consumption*

*5.4.Stable Nodes*

In our evaluation, Stable Nodes at moment is computed over the period from the beginning time (0) until a particular moment, it has been shown that (Fig.6) the total Stable Nodes in a ES-MHRT network is increased (7) compared to HYMN(6).

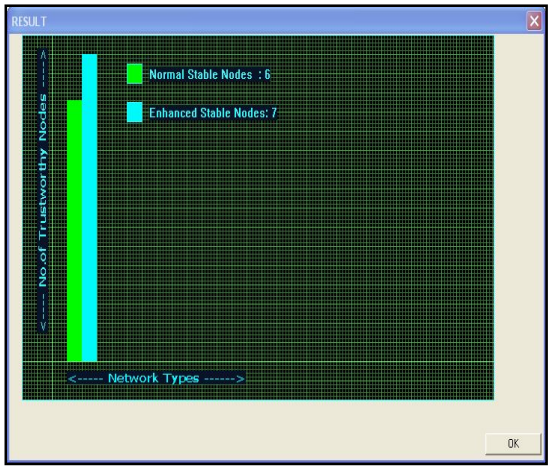


*Figure 6: Stable Nodes*

*5.5.Throughput*

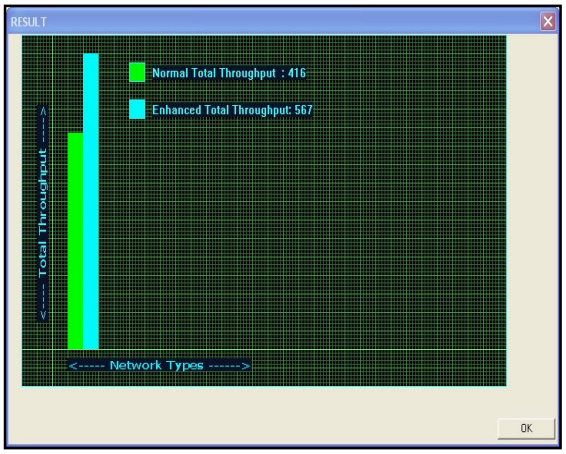


*Figure 7: Throughput*

In our evaluation, throughput at a moment is computed over the period from the beginning time (0) until that particular moment. Note that in our experiment (Fig.7) throughput is 567 for ES-MHRT and 416 for HYMN Throughput reflects how efficiently the network is collecting and delivering data.

**6.Conclusion And Future Work**

We designed and implemented ES-MHRT (Efficient Secured Multi-Hop Routing Technique), a robust trust aware routing framework for WSNs, to secure Hybrid multihop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information. However, from our experimental result, it is revealed that the sender understand the status of delivery report from receiver only, which costs more time to understand the reliable route. Thus Sender couldn't forward the data in fast manner, which affects the Network Performance in terms of Throughput and Bandwidth Utilization. This is the major issue.

**7.Reference**


1. Ahmed E.A.A. Abdulla, "HYMN: A Novel Hybrid Multi-Hop Routing Algorithm to Improve the Longevity of WSNs," IEEE Transactions On Wireless Communications, Vol. 11, No. 7, July 2012.
2. Guoxing Zhan, Weisong Shi, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2, March/April 2012.
3. Padmavathi, G., & Shanmugapriya, D.A survey of attacks, security mechanisms and challenges in wireless sensor networks. International Journal of Computer Science and Information Security (IJCSIS): Vol.4, No.1 & 2.2009.
4. Hanapi,. Z.M. Ismail,. M,. Jumari,. K. & Mahdavi,. M. Dynamic window secured implicit geographic forwarding routing for wireless sensor network. World Academy of Science, Engineering and Technology.2009.
5. Kavitha, T., & Sridharan, D.Security vulnerabilities in wireless sensor networks: a survey. Journal of Information Assurance and Security 5, (p31-44) .2010.
6. Unoma N. Okorafor, and Deepa Kundur, "Security-Aware Routing and Localization for a Directional Mission Critical Network" ieee Journal On Selected Areas In Communications, Vol. 28, No. 5, June 2010
7. R.A. Shaikh, H. Jameel, B.J. dAuriol, H. Lee, S. Lee, and Y. Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 20, no. 11, pp. 1698-1712, Nov. 2009.