Secure Routing in Wireless Sensor Network using HTARF

M.S.Krishnaveni[1], Dr.K.Kavitha[2]

1. M. Phil Scholar, Mother Teresa Women's University, Kodaikanal, India.
2. Assistant Professor, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, India.

Abstract *— A wireless sensor network (WSN) is a group of distributed sensor self organizing (managing) nodes. There different types of attacks (DOS, Sybil, stealthy, wormhole attack) that affects the security level of the network. Hence the security is the major issue of the WSN. To improve the security level of the network, the trust parameters should be implemented with energy conservation. Here HTARF (Hybrid Trust Aware Routing Framework) is implemented to improve the security level and lifetime of the network. In this paper HTARF algorithm and its uses are discussed. Through this algorithm energy awareness is established in network. HTARF algorithm provides trustworthable secure routing. The simulation analysis proposed here is based on three parameters are Energy Monitor, Trust Aware Manager and Distance Measurement Analyzer. This simulation analysis results are measured for the performance metrics (Packet Delivery Ratio, Latency, Energy Conservation, False Positive Rate and Detection Ratio). The Hybrid Trust Aware Routing Framework implementation in WSN provides better energy conservation, high packet delivery ratio and efficient security metrics.*

Keywords *— DOS, Energy Awareness, HTARF, Latency, Security, Trust Awareness, WSN.*

I. INTRODUCTION

Wireless sensor networks (WSNs) have been broadly utilized as a part of various fields, such as environment monitoring, health care monitoring, earth sensing, scientific observation, emergency detection, structure monitoring and intrusion detection [1]. There are many attackers to makes the sensor nodes to be misbehave and performs malicious functions. This affects the security and trust level of the network. In order the overcome this issue, wide variety of methods and techniques are proposed[4]. Trust management scheme and trust evaluation detects the malicious nodes. In this paper highly scalable cluster-based hybrid trust management protocol is used. This HTARF (Hybrid Trust Aware Routing Framework) protocol is effectively deals with selfish, Untrust or malicious nodes. This protocol implementation in the wireless sensor network establishes energy awareness and avoid the malicious nodes in the network. This increases the reliability, security level and trust level of the network. Data packet losing or dropping during data transmission is decreased. HTARF provides trustworthy and energy efficient route. In this paper the algorithm HTARF is discussed and explain how it works and work flow.

II. RELATED WORK

The primary purpose of trust-based routing protocol is to establish a trustworthy and efficient route between two nodes that can transmit data from the source to the destination. Routing algorithms determine the results of routing selection, which will directly affect the presentation of trust-based routing, such as network security, routing delay, and computational overhead. Accordingly, routing algorithm is one of the most important components in trust-aware routing protocols. Theodorakopoulos and Baras examine the effect of trust metric from the perspective of mathematical methods [2]. SAR is a secure routing protocol in WSNs that can determine the shortest path with desired security attributes [3]. Reputation broadcast (flooding mechanism) is another common method for receiving guidance from neighbors [5]. In [6], a trust-aware routing protocol (TARP) was proposed. Two steps are utilized to find a trusted neighbor node. The initial step, "One Hop Check" and will only be commenced by the source node that has some data to transmit. The source node will send a Neighbor Request to all its neighbors and ask them for their trust attributes. Once the trust attributes reaches the source node, then it will select the most trusted node. In step two, the source node will perform a credit check on the preselection node, it communicates directly with its neighbors. For this purpose, the source node will use a different channel and a temporarily higher energy than the one used in step one. The source node will send a far neighbor request to nodes. In this case, most of the neighbor nodes of preselection node will receive the call for (request) and response with a faraway neighbor reply. However, to implement this approach, frequency-hopping and time synchronization technologies are needed. These most difficult MAC scheduling mechanisms may limit the applications making it unattractive to WSNs.

III. HTARF DATA FLOW DIAGRAM

Initial stage is starts with implementing the sensor node in the routing the framework. To secure the WSNs against adversaries misdirecting the multihop

routing, have designed and implemented HTARF, a robust trust-aware routing framework for dynamic WSNs. The hybrid protocol that separates the network into several zones, which makes a hierarchical protocol. The condition applying to check secure routing. If it gets true then the network form a trustable route instead of checking attackers. Secure routing being faild it will check again and again for the Multi hop routing. Trust is introduced to prevent from various attacks and safely the Trust Based Effective Route Transmission performed. Trust mechanism secures data forwarding by isolating nodes with malicious intention using trust value on the nodes. Based on HTARF, we also demonstrated a proof-of-concept data packets dropped, providing reliable data transmission of wireless application.

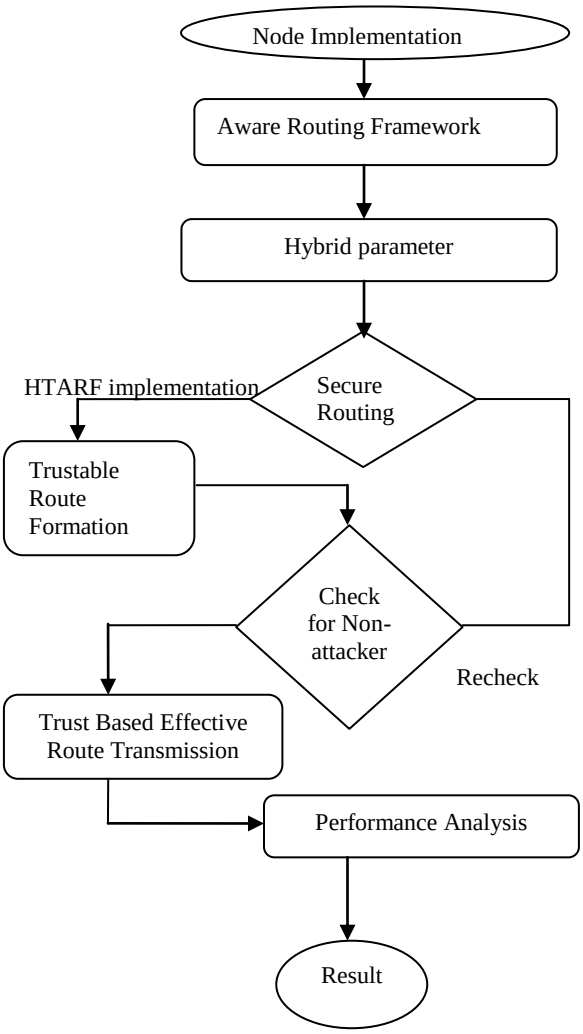

FIG. 1 HTARF DATA FLOW DIAGRAM

The first step is implementation of nodes and connected with links. Then the Aware routing framework is implemented. Next step is to form hybrid structure by clustering nodes. Cluster head is selected based on more number of links interconnected with neighbours. Members of the cluster is managed and evaluated by cluster head. Then the trust level is managed and evaluated by cluster head and form trustable routing to and fro base station. This step is Trustable Route Formation. HTARF implementation is performed by rechecking for the secure multi hop routing transmission. Next step is to transmit data or message by Trust Based Effective Route Transmission. Performance analysis is evaluated based on Packet Delivery Ratio, Latency, Energy Conservation, False Positive Rate and Detection Ratio. Finally result is generated.

IV. TYPES OF MESSAGE IN HTARF

There are four types of message defined in HTARF protocol.

A. *Route Request (REQ) Message*

It is used to establish a route to the final destination in WSN.

B. *Route Reply (REP) Message*

It is used to prepare routing table from destination to source node.

C. *Check For Trustable Route Message*

On the reception of this message the source node commence route discovery in the WSN for the destination node is an trustable path or not. User can send more messages according to the type of application.

D. *Route Failure (RTF) Message*

A node broadcasts this type of the message if the node fails to find a trustable path to communicate with all the nodes in the routing table.

V. SYSTEM MODULES

There are four modules node implementation, multi-hop routing in distributed WSN, data aggregation and clustering and HTARF implementation to design this system.

A. *Node Implementation*

Here we are implementing some sensor nodes with initial energy. These sensor nodes may request (call for) to transfer the data's as per our tcl script, so that we can trace the graphical output such as NAM, Graph.

B. *Multi-Hop Routing in Distributed WSN*

It is a distributed implementation in wireless sensor network (WSN). In WSN each sensor node has its own individual energy that preserves the connectivity of the network. Each sensor node has its neighbor node local information to do Multi-hop transmission. At Execution time in each round, a sensor node that decides to switch its status collects or updates the information of its Next-hop neighbors to find

replacement nodes. Quality shows better results, which achieves a longer lifetime.

C. *Data Aggregation and Clustering*

In the wireless network, cluster head is selected by the sensor nodes based on the link connectivity among the nodes. The nodes which have highest link connectivity when compared with its two-hop neighbors are selected as cluster head. These cluster heads transmits an advertisement message to all its neighboring nodes. The normal nodes have to trace the information that contained in the advertisement message. The advertisement message normally contains the cluster-head ID and information about the location of the cluster head. The normal nodes trace the information within their radio range.

Communication has to be distributed between the cluster head and normal nodes. For this, each normal node chooses one of the advertisement messages as its cluster head by means of powerful Received Signal Strength (RSS) and transmits a information (member message) back to the selected cluster head. The current energy status of the normal node and its ability of being a supportive node is added into the message. Also, the information related to reliability value, unreliable sensing count, reliable sensing count and hybrid trust value of the node are also added to the message. For the identification of the nearest neighbor cluster head, consider two cluster heads x and y. If an advertisement message signal is obtained at a cluster head x from another cluster head y, and y has a higher RSS value than the threshold value, then cluster head y will be considered as the neighbor cluster head and the ID of cluster head y is stored.

D. HTARF Implementation

HTARF identifies such trespassers by their low trustworthiness and routes data through paths avoiding those intruders to achieve satisfactory *throughput*. In addition to data package transmission, there are two varieties of routing information that need to be exchanged. They transmit messages from the base station about data release and energy cost description messages from each node. Neither communication needs acknowledgement. A broadcast message from the base station is busy to the whole network. The efficiency of a broadcast message is checked through its field of source series number. Then next another type of exchanged routing message is the energy cost details message from each node, which is broadcast to only its neighbors once. Any node getting such an energy cost report message will not forward it.

Neighbor: *F*or a node N, a neighbor (neighboring node) of N is a node that is accessible from N with one-hop wireless transmission.

Trust level: For a node N, the trust efficiency level of a neighbor node is a decimal number in [0, 1], represents N's opinion of that neighbor's level of reliability. Trust value is calculated by reliable and unreliable of the nodes For instance, the cluster have 5 sensor nodes i.e., n1, n2, n3, n4 and n5. Then the distance between the successive nodes is estimated as d1, d2, d3, d4 and d5. The average of the values is calculated, □ 1 and compared with threshold rate, N1 of the cluster. For instance, the clusters have 5 sensor nodes (n1, n2, n3, n4 and n5) and the difference between the successive readings of each node is r1, r2, r3, r4 and r5. Then the average value N2 of the readings is compared with its threshold value, N2 of the cluster. If N1>N1 and N2>N2, then the nodes are unreliable. If N1<N1 and N2<N2, then the nodes are reliable. Two counters called reliable sensing watcher and unreliable sensing watcher are maintained, for the values of N1 and N2. It indicates the reliability of the sensor node. The sensor nodes can be differentiated as malicious or compromised node based on the reliability factor. Thus it helps to maintain the network data away from that of the malicious nodes. This factor is estimated using the formula:

$$TTV = W1\ Ri + W2\ PDRi + W3\ RVi / W1 + W2 + W3$$

Energy cost: For a node N, the energy cost of a neighbor node is the average energy cost to successfully deliver a unit-sized data packet with this neighbor node as its next-hop node from N to the base station.

$$Etotal = Etrans + Erecie + Eprocess + Esense$$

Finally the total energy cost is calculated by the minimum of energy cost of the transmitting distance. The least distance of the member node to the cluster head is calculated and that is denoted by following equation

$$Min\ (Etotal)$$

Packet Delivery Rate Calculation: It gives the information related to the communication ratio. The egotism and the regularity (reliability) of the sensor nodes is indicated by this factor:

$$PDRi = STRi – PFRi / STRi + PFRi$$

Where,

PDRi = The packet delivery rate of the sensing count node I is $1 \leq i \leq k$

STRi = The success count of the packet delivery rate of the node i

PFRi = The failure count of the packet delivery rate of the node i

Power : The battery value represents the power in the nodes. Each sensor node broadcasts quantification value of its own Pi:

$$Pi : -1 \leq P \leq 1$$

The cluster head now evaluates the rank of the node in order to select the nodes for data Aggregation. For this purpose, hybrid protocol is used.

VI. CONCLUSION

In this paper, HTARF algorithm implementation is explained in detail.It provides better security for multi – hop routing transmission in WSN. It protects WSN against malicious function of nodes and severe attacks through dynamic replaying routing information. Trust management, distance measurement and energy cost detection of each node in network are estimated. Then performance metrics is evaluated based on the simulated and empirical test results of Packet Delivery Ratio, Latency, Energy Conservation, False Positive Rate and Detection Ratio.Finally result is generated. HTARF provides trustworthiness and energy efficiency. The efficiency of node can be easily estimated by adding additional data aggregation about each node's capacity. Hybrid rules are formed based on dynamic mobility of the nodes. Finally, we demonstrate a proof-of-concept mobility based target detection application using trust, energy cost and distance estimators that are formulated on top of the Hybrid TARF. The algorithm can be added to any existing routing algorithm for Trust and power management.

REFERENCES

[1] *https://en.wikipedia.org/wiki/Wireless_sensor_network*

[2] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 318–328, 2006. View at Publisher · View at Google Scholar · View at Scopus

[3] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks,"IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2–22, 2006. View at Google Scholar

[4] http://www.hindawi.com/journals/ijdsn/2014/209436/

[5] S. R. Zakhary and M. Radenkovic, "Reputation-based security protocol for MANETs in highly mobile disconnection-prone environments," in Proceedings of the 7th International Conference on Wireless On-demand Network Systems and Services (WONS '10), pp. 161–167, February 2010. View at Publisher ·View at Google Scholar · View at Scopus

[6] L. Abusalah, A. Khokhar, and M. Guizani, "Trust aware routing in mobile ad hoc networks," inProceedings of the IEEE Telecommunications Conference (GLOBECOM '06), pp. 1–5, December 2006.View at Publisher · View at Google Scholar · View at Scopus

[7] http://www.hindawi.com/journals/ijdsn/2014/209436/
.