ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 4, April 2016

Precising the Characteristics of Hybrid Trust Aware Routing Framework

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 remote sensor system (WSN) is a gathering of spatially disseminated self-governing sensors to screen physical or natural conditions (temperature, pressure, sound, etc.,) and to agreeably transmit their information through the system to a primary area. The modern networks are bi-directional, also enabling control of sensor activity. For establishing the security in the wireless sensor networks, [10] trust parameters can be incorporated in the network with energy conservation and Hybrid Trust Aware Routing Framework (HTARF) can be deployed. The HTARF algorithm can effectively find and successfully avoid the malicious nodes in the networks and also establish energy awareness in the networks. Moreover, the algorithm can decreases the number of data packets dropping, providing reliable data transmission [11]. The novel design implemented using HTARF is a strong trust aware routing framework for dynamic WSNs. HTARF provides trustworthable and energy efficient route. Most importantly, HTARF proves effective against those harmful attacks developed out of Identity deception. The flexibility of TARF is verified by extensive evaluating both simulation and empirical experiments on large scale WSNs. To secure the wireless sensor networks against adversaries misdirecting the multi -hop routing. The simulation analysis are proposed based on three trust parameters: Energy Monitor, Trust Aware Manager and Distance Measurement Analyzer and the simulation results are measured for the performance metrics: Packet Delivery Ratio, Latency, Energy Conservation, False Positive Rate and Detection Ratio. From the experimental analysis, Hybrid TARF has better energy conservation, high packet delivery ratio and better security metrics in terms of False positive rate and Detection ratio.**

***Index Terms*— Energy Awareness, HTARF, Security, Trust Awareness, WSN.**

I. INTRODUCTION

Wireless sensor networks (WSNs) have been broadly utilized as a part of various fields, such as environment monitoring, and intrusion detection. There are many factors make sensor nodes being more vulnerable and performs malicious functions. In order to address this issue, wide variety of schemes and methods are proposed. Trust evaluation and trust management plays critical and important role in detecting the malicious nodes. We propose a highly scalable cluster-based hybrid trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish, untrustful or malicious nodes. For establishing the security in the wireless sensor networks, trust parameters can be incorporated in the network with energy conservation and Hybrid Trust Aware Routing Framework (HTARF) can be deployed. The HTARF algorithm can effectively find and successfully avoids the malicious nodes in the networks and also establish energy awareness in the networks. Moreover, the algorithm can decreases the number of data packets dropped, providing reliable data transmission. The novel design implemented using HTARF is a robust trust aware routing framework for dynamic WSNs. HTARF provides trustworthy and energy efficient route.

II. RELATED WORK

The trust-based routing protocols have been proposed for the security and efficiency considerations in WSNs [1,2,3]. Paris et al. proposed a new cross-layer metric design called expected forwarding counter (EFW) for reliable routing in wireless networks. It motivates the cooperation between nodes and cope with the problem of selfish behavior. In [4], a bayesian game approach, which prevents DoS attacks is presented in WSNs. Then, a secure routing protocol is also proposed, it combines the bayesian approach with LEACH protocol. These routing protocols only aim at dealing with a particular attack, which is not enough to ensure the network security. Karlof and Wagner depicted the attacks against sensor networks and suggest solutions for secure routing [5], but they did not consider the effect of attacks on trust management systems.The solutions of some new attacks such as selfish and colluding attacks against trust evaluation were not discussed. Yu et al. examine many different attacks and countermeasures related to trust schemes in WSNs [6]. In any case, they simply categorized the various types of existing attacks and did not design secure routing protocols according to the analysis results.

III. PROPOSED SYSTEM

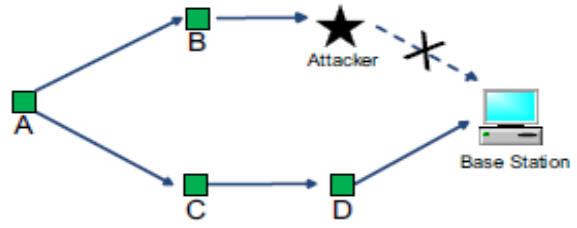
This is proposed Hybrid routing protocol (HRP) to decrease probability of failure nodes and to delay the time interim

before the expiry of the first node (stability period) and increasing the lifetime in heterogeneous WSNs, which is crucial for many applications. The sensor nodes are grouped into various clusters and each cluster has one elected cluster head. The cluster head initially evaluate the distance between each member and itself, by exchanging topology discovery packets. The cluster head collects the data from its members. Along with data, the each member attaches its current power level. Then the cluster head decide the trust level of each node by estimating the correctness of data. It can be estimated with the help of spatial and temporal changes (i.e.,) difference in two consecutive values and difference in readings of neighbor sensors.

To protect WSNs from the harmful attacks utilize the replay of routing information, we have designed and implemented a resilient trust-aware routing framework, TARF, to secure routing solutions in wireless sensor networks. Based on the distinctive characteristics of resource-constrained WSNs, the design of TARF centers on trustworthiness and energy efficiency. Though TARF a thorough and independent routing protocol can be developed, the purpose is to allow existing routing protocols to integrate our implementation of TARF with the least effort and thus producing a secure and efficient fully-functional protocol.

TARF does not requires tight time synchronization and known geographic information. Most importantly, TARF proves flexible under various attacks using the replay of routing information, which is not achieved by previous security protocols. TARF reveal steady improvement in network performance against strong attacks (sinkhole, wormhole, Sybil attacks). The effectiveness of TARF is demonstrate through extensive evaluation with simulation test and empirical method experiments on large-scale WSNs.

HTARF module is ready-to-use with low overhead, which as demonstrated can be integrated into existing routing protocols with simplicity; the revelation of a proof-of-concept mobile target detection program indicates the potential of HTARF in WSN applications.



An example to illustrate how *TrustManager* works.

IV. DESIGN OF HTARF

HTARF (Hybrid Trust Aware Routing Framework) secures the multi-hop routing in WSNs against intruders exploiting the replay of routing information by assessing the trustworthiness of neighboring nodes. It identifies such intruders that mislead noticeable network traffic by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. HTARF is also energy-efficient, highly scalable, and well adaptable. Before introducing the complete thorough design, we first introduce several necessary notions here.

A. *Neighbor*

For a nodeN, a neighbor (neighboring node) of N is a node that is connected with N and perform one-hop wireless transmission.

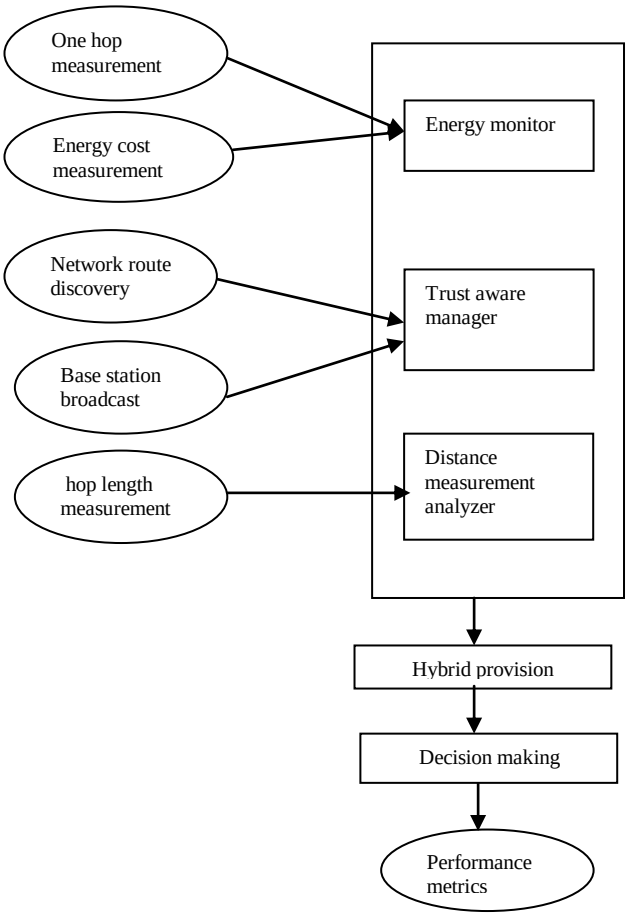
B. *Trust Level*

For a nodeN, the trust (reliability) level of a neighbor is a decimal number in representing N's opinion of that neighbor's level of reliability. Specifically, the trust (reliability) level of the neighbor is N's estimation of the possibility that this neighbor correctly distributes data reaches the base station. That trust level is denoted as T in this paper.

C. *Energy Cost*

For a nodeN, the energy cost of a neighbor is the average energy cost to successfully distribute a single unit data packet with this neighbor as its next-hop node, from N to the base station. That energy cost is denoted as E in this paper.

V. SYSTEM ARCHITECTURE



Energy monitoring services determine actual energy measuring the hop values and cost level. Trust Aware manager discovers Network path from base station. Using

Hop length measurement analysing distance between networks. Let it shows Hybrid provision wsn with obtained results, our hybrid approach outperforms in this schemes. Decision Making with HTARF integrates trustworthiness and energy efficiency in making routing decisions in trust-aware routing. The trust management assigns each node a trust value according to its reputation (past performance). Finaly get the performance for node transmission.

A. *Energy monitor*

The energy level of each and every node of the network is estimated by Energy Cost Measurement, then the hop value also evaluated by One Hop Measurement. The cost of energy to transmit data from one node to another sensor node is evaluated.

B. *Trust AwareManager*

The reliable network path is allocated from basestation. Network Route Discovery selects the trustable nodes to form the reliable network. Base station Broadcast distributes the data from base station through reliable nodes and decreases the packet dropping and improves security of the network. Trust level and security of the network can be managed and increased.

C. *Distance Measurement Analyzer*

The distance of the hop is measured. Through One Hop Measurement, the distance between the one node to another node (hop) is estimated.

D. *Hybrid Provision*

Data aggregation and clustering is implemented and follows the hybrid approach [8]. More than two nodes are clustered and the cluster head is selected by the sensor nodes based on the link connectivity among the nodes. The member nodes of the cluster is communicate with their cluster head and transmit data between member nodes and cluster head. The base station broadcast data through cluster head. Cluster head in the network monitors the trustlevel and energy cost of their each and every member nodes, then increases the trustlevel of the network.

E. *Decision Making*

Here efficient and secured network path is routed to transmit data. The selection is based on trustworthful, energy cost, reliable, lifetime of the sensor nodes and network path [9].

F. *Performance Metrics*

The performance of this system is evaluated based on energy efficiency, detection ratio, packet delay, packet delivery ratio. Positive rate will be evaluated by calculating the data bits transmission with time. Average residual energy is evaluated in terms to for transmission with its neighbor.

VI. CONCLUSION

To exploit the replay of routing information against harmful attackers and intruders, the proposed algorithm Hybrid Trust-Aware Routing Framework (HTARF) provides better security for WSN in multi-hop. For the survival of wireless sensor network under harsh and hostile environment, HTARF provides trustworthiness and energy efficiency. With the concept of innovative trust management, HTARF enables a node to keep track of the trustworthiness of its neighbors and there by select a reliable route path. Hybrid parameter TARF effectively protects WSN from severe attacks through dynamic replaying routing information. Without time synchronization and known geographic information, 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. The efficiency of node can be easily estimated by adding additional data aggregation about each node's capacity.

REFERENCES

[1] S. Paris, C. Nita-Rotaru, F. Martignon, and A. Capone, "EFW: a cross-layer metric for reliable routing in wireless mesh networks with selfish participants," in Proceedings of the IEEE INFOCOM, pp. 576–580, April 2011. View at Publisher · View at Google Scholar · View at Scopus

[2] K.-S. Hung, K.-S. Lui, and Y.-K. Kwok, "A trust-based geographical routing scheme in sensor networks," in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '07), pp. 3125–3129, March 2007. View at Publisher · View at Google Scholar · View at Scopus

3] M. E. Mahmoud and X. Shen, "Trust-based and energy-aware incentive routing protocol for multi-hop wireless networks," in Proceedings of the IEEE International Conference on Communications (ICC '11), June 2011. View at Publisher · View at Google Scholar · View at Scopus

4] M. Mohi, A. Movaghar, and P. M. Zadeh, "A bayesian game approach for preventing DoS attacks in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications and Mobile Computing (CMC '09), pp. 507–511, January 2009.

5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2-3, pp. 293–315, 2003. View at Publisher · View at Google Scholar · View at Scopus

6] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867–880, 2012.View at Publisher · View at Google Scholar · View at Scopus

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

8] F. BAO, R. CHEN, M. J. CHANG. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, IEEE Transactions on Network and Service Management, 9: 169-183, 2012.

[9] C.Wang, J. X. Yu, Q. Lin. A security wireless sensor network routing algorithm based on Credibility, Communications, 29: 105-112, 2008.

[10] Q. JING, L. Y. TANG, Z. CHEN. Trust management in wireless sensor networks, Journal of Software, 19: 1716-1730, 2008.

[11] G. YANG, S. YING, W. YANG. Reputation model based on behaviors of sensor nodes in WSN, Journal on Communications, 30: 18-26, 2009.