ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ENERGY TRUST CALCULATION FOR MALICIOUS FREE RELIABLE NETWORK

R.Sindhu [*], G.Swaminathan

[*] Department of CSE, Mount Zion College of Engg & Tech, Pudukottai, Tamilnadu, India
Department of CSE, Mount Zion College of Engg & Tech, Pudukottai, Tamilnadu, India

ABSTRACT

Wireless sensor networks (WSNs) have recently gained a lot of attention by scientific community. Small and inexpensive devices with low energy consumption and limited computing resources are increasingly being adopted in different application scenarios including environmental monitoring, target tracking and biomedical health monitoring. In many such applications, node localization is inherently one of the system parameters. Localization process is necessary to report the origin of events, routing and to answer questions on the network coverage, assist group querying of sensors. In general, localization schemes are classified into two broad categories: range-based and range-free. However, it is difficult to classify hybrid solutions as range-based or range-free. In this paper make this classification easy, where range-based schemes and range-free schemes are divided into two types: fully schemes and hybrid schemes. Moreover, comparing the most relevant localization algorithms and discuss the future research directions for wireless sensor networks localization schemes.

KEYWORDS: Wireless Sensor Network, Medium Access Control, Public key Infrastructure, Denial of Service.

INTRODUCTION

With the recent advancements in sensor technology, wireless communications, and embedded system, witness a rapid growth in the number of sensing capable devices connected to the Internet. The needs for mobility and convenience access also promote the use of wireless for the Internet connection. These recent developments have made wireless sensor network (WSN) one of the most important network technologies in Internet of Things (IoT).A practical WSN for IoT must be capable of rapid deployment and self-organization to perceive the physical world at anywhere and anytime. With the research efforts and contributions, WSNs have become an attractive platform for many applications.

Finally, the sensor nodes deployed in an unattended area may be compromised by adversaries through physical means. Once the keys are leaked, all the security mechanisms immediately become ineffective. In other words, cryptographic mechanisms are vulnerable to attacks launch internally. Due to the low complexity computation and high resistance to the internal attacks, trust evaluation is an effective solution to the above-mentioned issues in the public key infrastructure (PKI). Consequently, trust plays an important role in security mechanisms for WSNs. Although there are different definitions for trust in the previous works, the trust of nodes is normally composed of direct trust and indirect trust. The direct trust is based on direct observations of each node that participates in data communications, and the indirect trust is obtained from recommendations of other nodes. Besides, the trust evaluation process can also be divided into two parts: 1) trust derivation and 2) trust computation.

In order to minimize the management overhead of the network, an unweighted node evaluation scheme Node Evaluation with Assistant Trust (NEAT) is proposed to assist the central node (the initiating node of trust assessment) with evaluating its neighboring nodes' trust. When the central node wishes to evaluate a neighboring node's trust, it will query its assistants about this neighboring node. The assistants will then provide the queried node's trust values in their individual communities to the central node.

In the proposal, trust information is encapsulated in a route request packet which could exploit the reserved field. Together with the routing information, the route request packet is then broadcast to all neighbors. Once the packet is received, the neighbors look for the presence of the mentioned reputation option by checking the reserved field. If the node presented in the reputation option does not belong to the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

neighbors of the receiving node, it disregards the reputation information and leaves it unmodified in the forwarded route packet.

With the open and remote deployment environment, WSNs are generally vulnerable to various attacks, such as black hole attack, wormhole attack, and Sybil attack. In this approach, we assume that all the sensor nodes are compromisable. Compared with them, the sink node can be recognized as a highly trusted party in most cases with more sophisticated hardware. The attacks launched by malicious nodes can be divided into two types: 1) passive and2) active. In passive attacks, malicious nodes may passively gather sensitive information or behave elfishly in collaborative operations, such as routing, in order to affect the proper operation of WSNs. In active attacks, malicious nodes may actively request for sensitive information, influence the behavior of surrounding nodes, or directly affect the normal operation of WSNs using attacks such as denial of service (DoS).

Trust model essentially performs trust derivation, computation, and application. In this paper, we adopt watchdog as the foundation of detection mechanisms. Each sensor node is responsible for monitoring the behavior of its neighbors within its radio range. The detection results are utilized for the evidence of trust computation. The trust of an arbitrary node includes direct trust and indirect trust. Finally, the results of trust computation can be used as a measure of security for various aspects of communications.

Network

In this approach, WSN consisting of a fews in knodes and a number of sensor nodes that are randomly distributed in a designated area. Each sensor node is in charge of both detecting events and forwarding packets. All the sensor nodes are resource-constrained and have the same limited radio coverage. Consequently, end-to-end communication in a WSN is normally achieved via multihop relaying where a communication path is established in a distributed manner.

Security

With the open and remote deployment environment, WSNs are generally vulnerable to various attacks, such as black hole attack, wormhole attack, and Sybil attack. In this approach, we assume that all the sensor nodes are compromisable. Compared with them, the sink node can be recognized as a highly trusted party in most cases with more sophisticated hardware. The attacks launched by malicious nodes can be divided into two types: 1) passive and2) active. In passive attacks, malicious nodes may passively gather sensitive information or behave elfishly in collaborative operations, such as routing, in order to affect the proper operation of WSNs. In active attacks, malicious nodes may actively request for sensitive information, influence the behavior of surrounding nodes, or directly affect the normal operation of WSNs using attacks such as denial of service (DoS).

Trust Derivation

Trust model essentially performs trust derivation, computation, and application. In this paper, we adopt watchdog as the foundation of detection mechanisms. Each sensor node is responsible for monitoring the behavior of its neighbors within its radio range. The detection results are utilized for the evidence of trust computation. The trust of an arbitrary node includes direct trust and indirect trust. Finally, the results of trust computation can be used as a measure of security for various aspects of communications.

LITERATURE REVIEW

This section literature review has provides an overview and a critical evaluation of a body of literature relating to a research problem. Literature review is the most important step in software development process.

On Trust Models and Trust Evaluation Metrics for Ad hoc Networks

This paper presents [1]; security is one of the main challenges for the practical implementation of IoT, especially for a WSN-based IoT. Highly constrained devices will be the most vulnerable, and malicious entities will seek to control at least some devices either directly or indirectly. The first effort make all objects secure by default. The second effort is to give all IoT objects the ability to know the state of the network and its services. Objects should be able to use intrusion-detection systems and other defensive mechanisms to ward off attackers. Once an attack affects their services, IoT elements should be able to act quickly to recover from any damage. Such elements can use feedback from other mechanisms and IoT entities to map the location of unsafe zones, where an attack has caused service outages and trusted zones areas with no service.

Designing and Deploying Building-wide Cognitive Radio Network Testbed

According to this paper [2], data aggregation is necessary for extending the network lifetime of wireless sensor nodes with limited processing and power capabilities, since energy expended in transmitting a single data bit would be at least several

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

orders of magnitude higher when compared to that needed for a 32-bit computation. Reducing the amount of data transmission and rending energy savings. A similar estimator at the next hop node or base station reconstructs the original data. This approach tries to extend the network lifetime but it does not achieve.

A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory

This paper focuses on [3], trust evidence may be uncertain and incomplete. Using the theory of semi rings, show how two nodes can establish an indirect trust relation without previous direct interaction.. Malicious node cannot measure, so attackers easily hack the message in the network. The aim is to establish an in direct relation between two users that have not previously interacted; this is achieved by using the direct trust relations that intermediate nodes have with each other. There is no centralized PKI, Certification Authorities, or Registration Authorities with elevated privileges.

A new data aggregation scheme via adaptive compression for wireless sensor networks

In this paper [4], the topological structures related to trust metrics are more complicated. Trust-based routing is restricted by the physical conditions as well as trust conditions, and therefore requires a new routing algebra. Lastly, different groups of people may have different rules to establish and handle trust, and therefore, trust metrics are group dependent and non-uniform. When an end-to-end communication runs across multiple groups, more effort needs to be made to model the inter-operation between different trust-based routing protocols. Local monitoring schemes like Watchdog and Path rater and physical contact scheme have been proposed to collect the first-hand trust evidence. Trust-based routing is differentiated from traditional routing by introducing trust inference as one of important preprocessing for path selection and packet forwarding, and therefore should be explicitly.

A formal study of trust-based routing in wireless ad hoc networks

According to this paper [5], secure data aggregation is a challenging task in Wireless Sensor Network. This issue needs to be overcome using efficient technique. The Sensor Nodes death frustrates and the problem gets aggravated if the cluster node fails. When a cluster node fails because of energy depletion an alternative cluster needs to be chosen for that particular region. In periodical time each sensor node in the cluster should possess the next cluster head re-election based on energy to avoid node failure. Try to improve the throughput with reduced pack drop and also less energy consumption.

Localized geographic routing to a mobile sink with guaranteed delivery in sensor networks

In this paper [6], Integrated Location Service and Routing (ILSR) scheme, based on the geographic routing protocol GFG, for data communications from sensors to a mobile sink in wireless sensor networks. The objective is to enable each sensor to maintain a slow-varying routing next hop to the sink rather than the precise knowledge of quick-varying sink position. In ILSR, sink updates location to neighboring sensors after or before a link breaks and whenever a link creation is observed. Location update relies on flooding, restricted within necessary area, where sensors experience (next hop) change in GFG routing to the sink. Dedicated location update message is additionally routed to selected nodes for prevention of routing failure.

PROPOSED APPROACH

In this approach, the classification of localization algorithms based on the dependency of the range measurements easy with a focus on the hybrid algorithms; this classification is proposed also to help in comparing localization schemes. For example, hybrid range-based schemes perform more accurate than the fully range-based schemes. And a comparative study of existing localization algorithms from different perspectives is discussed in detail. In this paper, range-based schemes and range-free schemes can be divided into two sub categories: fully schemes and hybrid schemes. This classification is based on the dependency of the methods used and has a direct impact on the estimation of unknown node location. For example, there is schemes use at the same time range-based and range-free mechanism. According to the definition of range-based schemes mentioned above, if the schemes use range measurement techniques they are considered as range-based schemes, and if not they are considered as range-free schemes. Thus the hybrid schemes that combine range-based and range-free mechanisms are considered as range-based schemes. Range-based or range- free schemes may or may not use anchor nodes, i.e., anchor based or anchor free. The anchor-free schemes do not assume any node positions are initially known. While, the anchor-based schemes need some nodes aware of their positions called anchor nodes to provide geographic information to unknown nodes to localize. A promising method is to use mobile anchor node instead of static anchor

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

nodes. A mobile anchor node is aware of its position, and moves in sensor area and broadcasts its current position periodically to generate a number of virtual anchor nodes. The unknown sensor nodes estimate their locations by measuring the geographic information of the virtual anchor nodes. The present advantage in our system is a) It enable disconnected mobile nodes to rejoin the network within a short time and avoid the accumulative data loss. b) CBR (Cluster Based Routing) Mobile has the added values of high bandwidth utilization of the networks. c) To avoiding network traffic. d) To consume the energy level of the process. e) Best transmission range on the networks.

SYSTEM DESIGN

System Architecture

Generally algorithms shows a result for exploring a single thing that is either be a performance, or speed, or accuracy, and so on. In this protocol, a source can find trusted paths to a destination in a single route discovery round. New route discovery is needed only when all paths break or fail to meet the trust requirement. This protocol provides a flexible and feasible approach to choose a trusted path and the routing protocol is tested against denial of service attack. This system can be extended to defend against several attacks and finding secured paths. Again this can be extended to find shortest path from the list of multiple path. Multiple paths can also be used to balance load by forwarding data packets on multiple paths at same time.

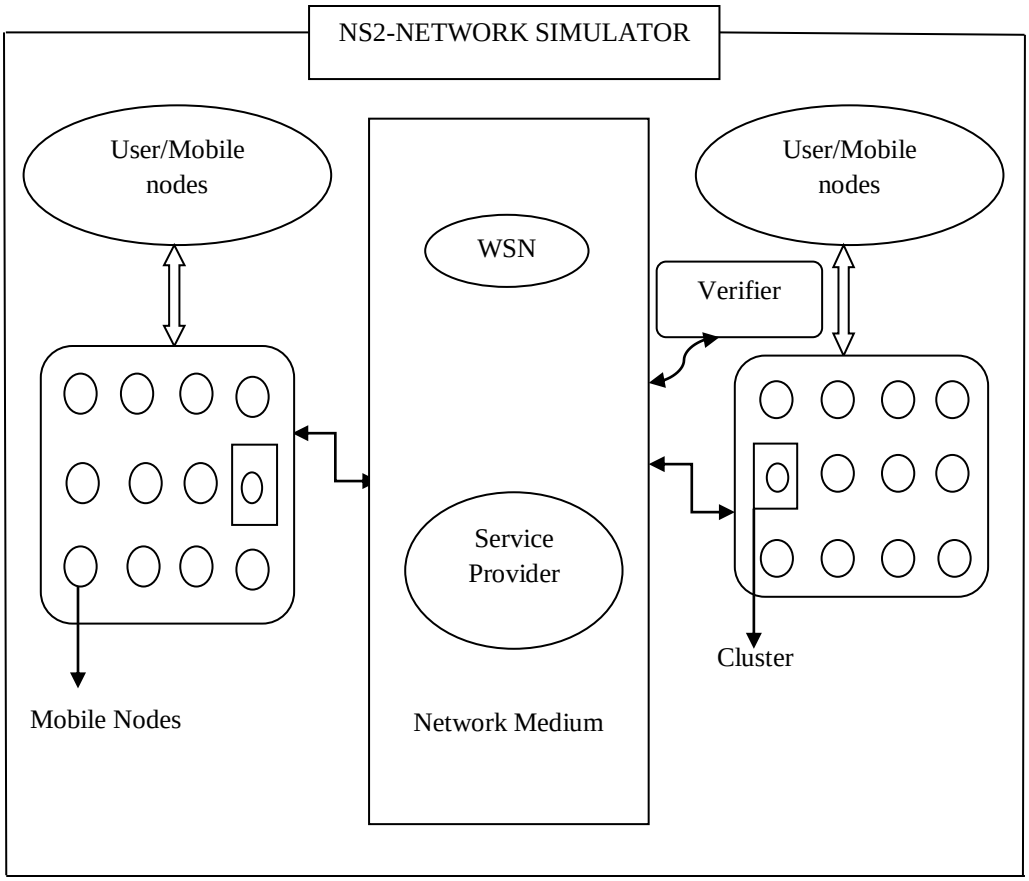

Fig 1: System Architecture

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Modules

1. Network Initialization
2. Trust Calculation
3. Trust with Localization
4. Detection of Malicious Nodes
5. Performance Analysis

Network Initialization

Create a base wireless adhoc network with 30-40 numbers of sensor nodes and transfer data packets from sender node to receiver node with clustering using any of the clustering algorithms that involves the cluster head election algorithm Analyzing the nodes based on the behavior simulating the behavior of the normal node, malicious node and verifiers implementing an (DDOS) attacker node by changing its behavior into sensor network and transfer data packets from sender node to receiver node.

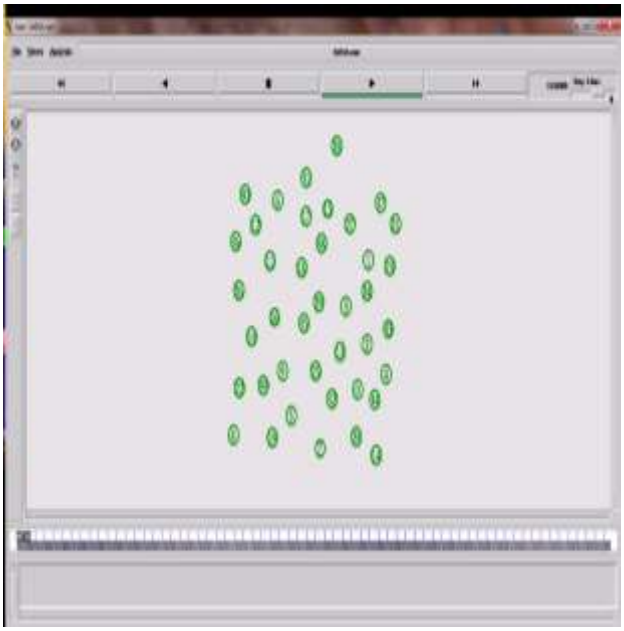

Fig 2: Network Intialization

Trust Calculation

Trust calculation is based on direct and indirect trust. When an event of broad casting of messages in cluster takes place the trust calculation has to been done and it should show all the trust nodes and message has to be broadcasted to all trusted nodes. The receiver takes the messages other nodes they will discard the broadcast message.

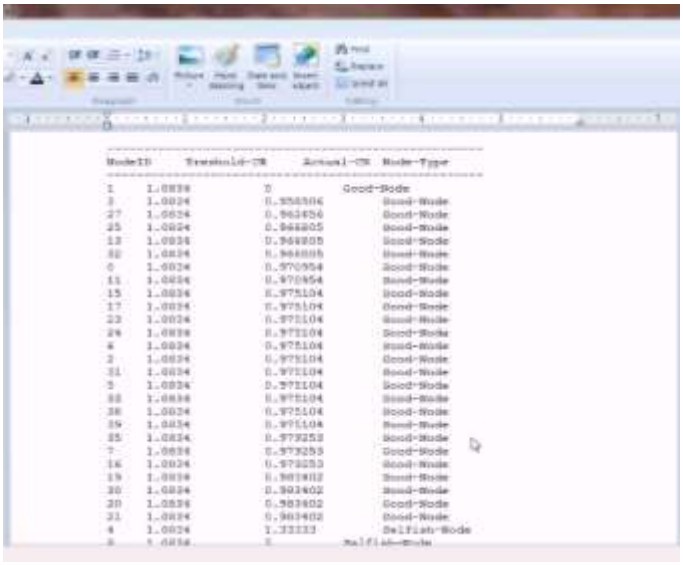

Fig 3: Trust Calculations

Trust with Localization

The concept of trustworthiness with localization to calculate the range based movement of the sensor nodes in order to identify the selfish nodes and existence of duplicate node based on the node ids. And system also dynamic in nature where the node behavior is computed with the time localization

Detection of Malicious Nodes

With trust and localization the malicious nodes should be detected and it is resilient to replication attack and DOS.

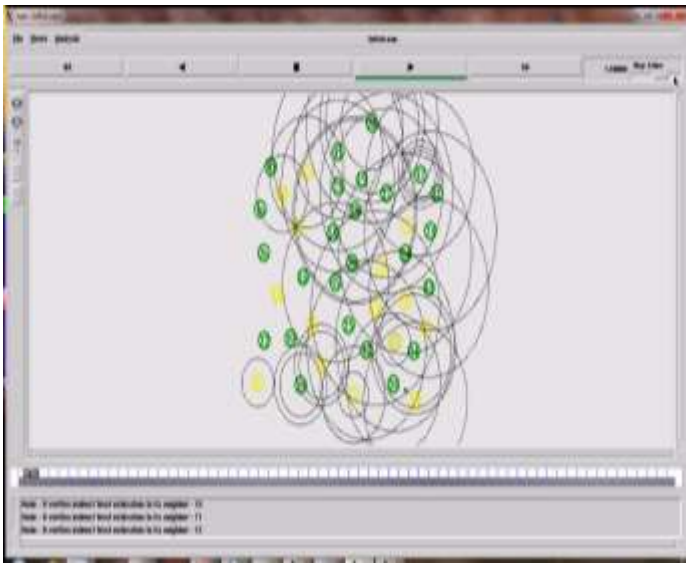

Fig 4: Malicious Nodes

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Performance Analysis
Performance analysis is done for security trade off, cost estimation, and complexity of operation.

CONCLUSION
Localization in wireless sensor network is a hot area of research that has been addressed through many proposed schemes. Based on the dependency of the range measurements theses proposal schemes are classified into two major categories: range-based schemes and range-free schemes. However, it is difficult to classify hybrid schemes which combine different methods based on connectivity information and/or range measurement techniques as range-based or range-free schemes. In this paper we make the classification of any localization schemes easy, where range based schemes and range-free schemes are divided into two types: fully schemes and hybrid schemes. Furthermore, this classification is proposed also to help in comparing localization schemes in terms of accuracy. In particular, between the schemes of the same category either for range- based or for range-free categories.

Acknowledgements
We would like to sincerely thank Assistant Prof. G.Swaminathan for his advice and guidance at the start of this article. His guidance has also been essential during some steps of this article and his quick invaluable insights have always been very helpful. His hard working and passion for research also has set an example that we would like to follow. We really appreciate his interest and enthusiasm during this article. Finally we thank the Editor in chief, the Associate Editor and anonymous Referees for their comments.

References
[1] G. Theodorakopoulos and J. Baras, "On trust models and trust evaluation metrics for ad hoc networks," IEEE J. Sel. Areas Communication, vol. 24, no. 2, pp. 318–328, Feb. 2006.

[2] T. Newman, S. Hasan, and D. DePoy, "Designing and deploying a building-wide cognitive radio network testbed," IEEE Communication. Mag., vol. 48, no. 9, pp. 106–112, Sep. 2010. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," Computer, vol. 44, no. 9, pp. 51–58, 2011.

[3] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," Sensors, vol. 11, no. 2, pp. 1345–1360, 2011.

[4] P. Kasirajan, C. Larsen, and S. Jagannathan, "A new data aggregation scheme via adaptive compression for wireless sensor networks," ACM Trans. Sensor Networks., vol. 9, no. 1, pp. 1–5, 2012.

[5] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[6] X. Li, J. Yang, A. Nayak, and I. Stojmenovic, "Localized geographic routing to a mobile sink with guaranteed delivery in sensor networks," IEEE J. Sel. Areas Communication, vol. 30, no. 9, pp. 1719–1729, Oct. 2012.

[7] V. Kapnadak, M. Senel, and E. Coyle, "Distributed iterative quantization for interference characterization in wireless networks," Digit. Signal Process, vol. 22, no. 1, pp. 96–105, 2012.

Author Biblography

Sindhu.R is currently a PG scholar in Computer Science and Engineering from the Department of Computer Science at Mount Zion College of Engineering and Technology, Pudukkottai. She received his Bachelor Degree in Information Technology from Kurinji College of Engineering and Technology, Tiruchirappallai and Tamilnadu. Her Research areas include Wireless Sensor Networks, Data warehousing and Distributed Computing.

Swaminathan.G is currently working as an Asst. Professor from the Department of Computer Science and Engineering at Mount Zion College of Engineering and Technology, Pudukkottai. He received his Bachelor Degree from Bharathidasan University, Tiruchirappalli and Tamilnadu and Master Degree from Prist University, Tiruchirappalli and Tamilnadu. His main research interests lie in the area of Distributed Computing, and Wireless sensor networks.