NETWORKING: ENHANCING PERFORMANCE MEASURES IN ENERGY EFFICIENT TRUST SYSTEM THROUGH WATCHDOG OPTIMIZATION FOR WIRELESS SENSOR NETWORK

Mr. S. Ramalingam, ME.,
Assistant Professor,
Computer Science and Engineering,
MRK Institute of Technology,
Kattumannarkoil, Tamil nadu.

Ms. R. Bhuvaneswari, ME,
Computer Science and Engineering,
MRK Institute of Technology,
Kattumannarkoil, Tamil nadu.
rbhuvanas1992@gmail.com,

ABSTRACT

Watchdog mechanism is one of the intrusion detection techniques in Wireless Sensor Network. The main purpose of this method is reducing the energy consumption as a key factor and also minimize the energy cost of watchdog usage while keeping the system's security in sufficient level. Then, I introduce an analytical model to evaluate the detection time and the cost of this collaborative approach. Sensor nodes are usually equipped with limited battery and work in an unattendive mode for long period of time such as the deep desert and ocean abyss. So Rechargement or replacement of those node's power very expensive and difficult. A way to reduce the detection time of nodes in a network is the collaborative watchdog and optimize watchdog frequency and reduce its redundancy. Finally determined trustworthiness and untrustworthiness node.

Index Terms – Wireless Sensor network security; Trust system; Energy efficiency; Watchdog technique;

I. INTRODUCTION

Watchdogs are used to detect trusted nodes in computer networks. A way to reduce the detection time and to improve the accuracy of watchdogs is the collaborative approach. A collaborative watchdog based on contact dissemination of the detected trusted nodes. In this context, there is a need for enhancement thorough investigation of the trust and reputations of sensors involved in data acquisitions, processing and communication.

The traditional approaches are not suitable to deal with node misbehaviour attacks due to resource-constrained nature of Manet and, the extensive computations and processing requirements of these approaches. The discovery of the data route might have some malicious nodes

that drop packets and lead to network malfunctioning.

The trust aware routing schemes have been proposed to deal with misbehaving of nodes in recent years, but neglect, false reporting, node residual energy level to avoid early depletion and overcome the traffic load. A way to reduce the detection time of trusted node (or non-cooperative) nodes in a network is the collaborative watchdog.

1) I conduct a novel study to reveal trust energy conflict induced by the inefficient use of watchdog techniques in existing WSNSs.
2) I optimize watchdog techniques in two levels, both of which consist of a theoretical analysis to show potential optimal results and a practical algorithm to efficiently and effectively schedule watchdog tasks.
3) It evaluates our optimization techniques using extensive experiments in a WSNET simulation platform and an in –door testbed in our collaborative lab.

Although sensor nodes which are located more closely may consume less energy to monitor each other due to shorter communication distance, These nodes are more likely of being compromised together and launch collaborative attacks.

II. RELATED WORK

A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. A price-based system uses virtual cash to control the transactions of a packet forwarding service. Although these two kinds of systems have been widely used, very little research has been devoted to investigating the effectiveness of the node cooperation incentives provided by the system [2] [3] [7]. A price-based system uses virtual cash to control the transactions of a packet forwarding service. Although these two kinds of systems have been widely used, very little research has been devoted to investigating the effectiveness of the node cooperation incentives provided by the systems.

In this enhancement, we use game theory to analyze the cooperation incentives provided by these two systems and by a system with no cooperation incentive strategy [1] [7]. We find that the strategies of using a threshold to determine the trustworthiness of a node in the reputation system and of rewarding cooperative nodes in the price based system may be manipulated by clever or wealthy but trust nodes. Illumined by the investigation results, we propose and study an integrated system [5] [6] [1] [3].

Position based opportunistic routing mechanism which can be deployed without complex modification to MAC protocol and achieve multiple receptions without losing the

benefit of collision avoidance. Opportunistic routing can still be achieved while handling communication voids [6] [4] [2].

Sink visits a point for data collection which can be few hops away from the node and the data has to be sent through other nodes. In these cases the intermediate nodes should not be able to read the transmitted information [1] [5] [3]. Data confidentiality also prevents the read only adversary from reading the stored data in the compromised node's memory [2] [14] [6]. Data integrity protects against unauthorized alteration of the data. Data integrity can be achieved only if the network has the ability to detect the manipulations done to the data by unauthorized parties, i.e., insertion, substitution and deletion. An encryption based symmetric cryptography is used to detect the misbehaving node in the sensor network [5] [3] [7].

Authentication applies to both nodes and data. It ensures the identity of the node with which it is communicating i.e., the two communicating parties can identify each other [6] [4] [7]. Information delivered through the network should be authenticated with respect to the generation time, date of origin, origin etc., and Data origin authentication also provides data integrity as the message modification can be detected[1][4][6].

In mobile ad hoc networks (MANETs), tasks are conducted based on the cooperation of nodes in the networks. However, since the nodes are usually constrained by limited computation resources [1] [4] [2]. trust nodes may refuse to be cooperative. Reputation systems and price-based systems are two main solutions to the node noncooperation problem. A reputation system evaluates node behaviours by reputation values and uses a reputation threshold to distinguish trustworthy nodes and untrustworthy nodes [3] [7] [5] [6].

III. EXISTING SYSTEM

Sensor nodes are usually equipped with limited battery and work in an unattended mode for a long period of time to adapt various harsh environments such as the deep desert and ocean abyss. Rechargement or replacement of those nodes' power is very difficult and expensive. So energy saving in WSN is crucial.

The energy consumption and network lifetime of WSNs are interdependent. It required more energy for processing of data whereas more for transfer of data from sensor to other. When all the nodes start detecting an intruder and transfer information to base station a large amount of energy consumed, and network lifetime reduced.

Data communication between source and destination is defined in single routed path.

IV. PROPOSED APPROACH

The ultimate goal is to reduce the energy consumption induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level. Sensor nodes

which are located more closely may consume less energy to monitor each other node.

Watchdogs are used to detect untrusted nodes in computer networks. A way to reduce the detection time and to improve the accuracy of watchdogs is the collaborative approach.

Data communication between source and destination is defined in multiple routed path. we optimize watchdog frequency and reduce its redundancy. Finally determined trustworthiness and untrustworthiness node.

A collaborative watchdog based on contact dissemination of the detected trusted nodes. Then, we introduce an analytical model to evaluate the detection time and the cost of this collaborative approach. A way to reduce the detection time of trusted node (or non-cooperative) nodes in a network is the collaborative watchdog.

V. EVALUATION

Watchdog Optimization Techniques

Watchdog is one of the intrusion detection techniques. Which is mainly used to detecting malicious node and also saving energy cost while keeping the system's security in maximum level. It is also used to detect untrust nodes in computer network and also reduce the detection time of malicious node.

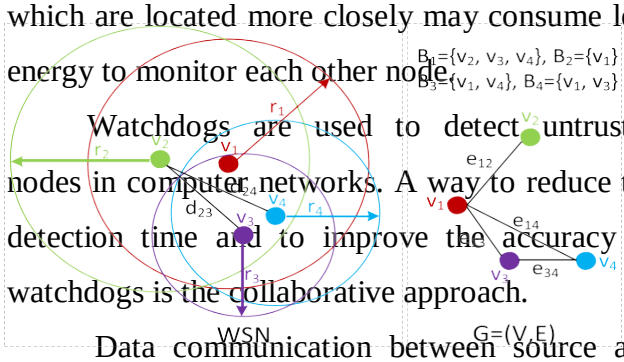


Fig 1: An example of WSN and the system model *G*

Energy Efficiency Model

In existing approach, to detect malicious node takes lot of energy consumption. Energy efficient trust mechanism for wireless sensor network by considering the identified vulnerabilities and defending approaches.

To estimate energy consumed by each watchdog task wtij , we follow a typical free space wireless radio model, which is widely adopted by the literature .In this model, a sensor node's transmitter unit consists of a transmit electronics device and a power amplifier, both of which will consume energy when transmitting signals.

In contrast, a node's receiver unit only consumes energy due to the receive electronics device. We follow prior research to assume that a proper power controller has been deployed to adjust transmit power amplifier according to the transmission distance.

Let be the energy consumed by a sensor node's transmit electronics (or receive electronics) when sending (or receiving) 1 bit information (measured in J/bit). Let _ be free space constant

measured in J/bit/m2. Then it can calculate the energy consumption when VI transmits 1 bit information to its neighbour node v j (dij ≤ RI).

We define $S_i(T)$, the staleness of table T_i at time T, to be the difference between and the freshness of T_i

$$S_i(T) = T - F_i(T)$$

$$\Pr[v_i \in A | v_j \in A](\infty)$$

Basic Algorithms

The Distance based Brobabilistic Algorithm (DBP) algorithm orders released nodes by proximity to their deadlines. DBP is known to be an optimal hard real-time probabilistic algorithm for detecting malicious node track (w.r.t. maximizing the number of nodes that meet their distance), if the nodes are preemptible .Since our nodes are prioritized, using DBP directly does not result in the best performance. Instead we use one of the following basic algorithms.

Heuristic Watchdog Frequency Adjustment Algorithms (HWFA) orders nodes by their priorities, breaking ties by distance. Our model does not directly have distance, but they may be estimated as follows: For each node ni, we define its release time ri as the last time Ti's freshness delta changed from zero to nonzero (i.e., the last arrival of new data in case of base tables, or, for derived tables, the last movement of the trailing edge point of its source tables). Then, we estimate the distance of Ji to be RI þ Pi (recall that the period of a derived table is the maximum of the periods of its descendants).

$$\text{Energy saving} = \frac{\text{Cost (Baseline)} - \text{Cost (WO)}}{\text{Cost (Baseline)}}$$

Trust Model

In this paper, we model the trust of a sensor node as this node's expected behavior distribution over time. The behavior could be data sensing or routing behavior etc. This trust model can allow our analysis to be focused on WSNTS's foundation, and will not be affected by higher level's trust update and aggregation processes.

This model, introduce three concepts. One is ***trustworthiness*** that can be used to estimate a sensor node's behavior. The other two are ***trust accuracy*** and ***trust robustness***, which can be used to measure how accurate the target nodes' trustworthiness can be recovered in the presence of WSN attacks and WSNTS attacks respectively.

The trustworthiness that the trust systems need to calculate at run time, the trust accuracy and trust robustness are two performance indices that we can use to evaluate and compare different trust systems' security levels. Trust systems do not need to compute the trust accuracy and robustness at run time.

Watchdog Frequency Optimization

A quality output is one, which meets the requirements of the trust node. And clearly presents the reduce the energy consumption of watchdog usage and also increase the lifetime of our wireless sensor network devices while keeping the system's security in sufficient level. It is most important to detect malicious node in specified routed path.

The data communication between source and destination is defined in multiple routed paths. It is design an efficient trust based routing protocol to deal with malicious node in the network which leads to false reporting and packet dropping.

It is used to implement and test proposed trust based routing protocol to overcome the traffic load and trusted nodes re-route the traffic through alternate path if active path is faulty or congested and is to develop a routing protocol that considers the node residual energy level to avoid early depletion of trusted nodes.

TABLE I
Notations Used in This Paper

Notations	Definitions
G=(V,E)	An undirected graph used to model a WSN
v_i	$v_i \leq V$ represents a sensor node in WSN
r_i	v_i 's communication range
d_{ij}	The special distance between vi and v_j
B_i	The set of v_j's neighborhood nodes
W_j	The set of v_j's watchdog nodes
Q_{ij}	The distribution of I_{ij}^t set
f_{ij}	Watchdog frequency v_j uses to monitor v_i
f_{nj}	A sensor node vj's normal behavior frequency
μ	Used by HWFA(E) algorithm to keep watchdog redundancy

VI. EXPERIMENTAL RESULTS

Watchdog frequency is the multi-step process that focuses on data structure software architecture and interface between nodes. The design process also translates the packets into the presentation of network that can be accessed for energy efficient.

WSNET Simulation

WSNET is an event driven module based WSN simulation framework. Start with sender. The sender sends Hello packets for all the nodes in the network to check whether all the nodes are an activation or not. Incase if some nodes are does not in activation, then it activate that node . For example, let assume one sender with two receiver sender[11],receiver[21],[33] respectively.11,21,33 denotes node's position. Then we define routed path using topology formation. After that, packet will be transformed to node by node.

Some nodes are forwards the packets to another node but few nodes are does not forward the packets to another node. It is called malicious node.

Node Creating

This module is developed to node creation and more than 30 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

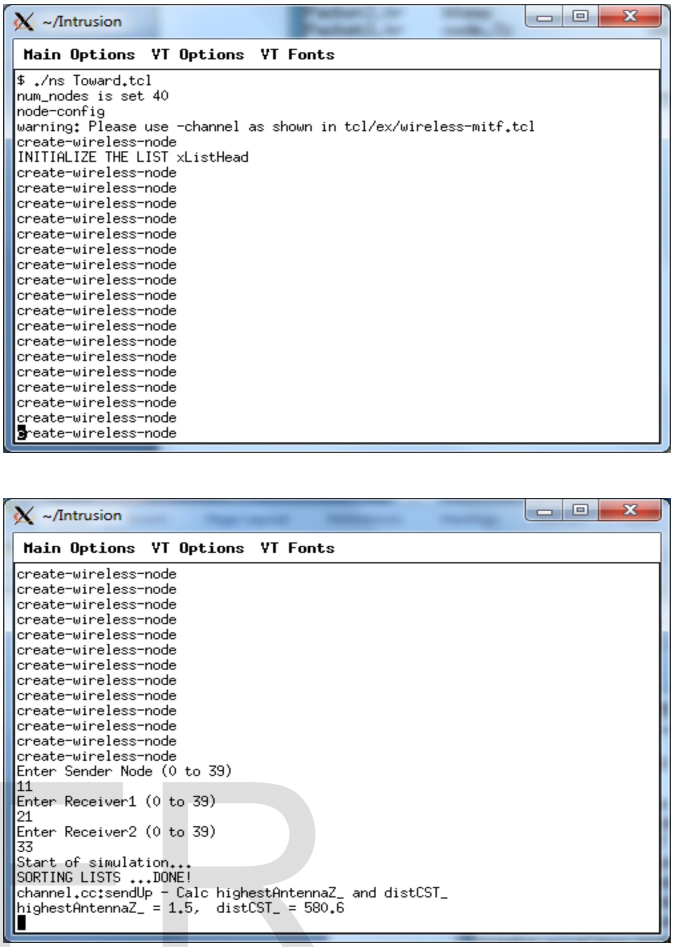


Fig 2: Node Creation

Node Configuration Setting

The sensor nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes. Fix the configuration to all of the nodes in communication network.

Detecting Untrust Node

Detection of trust node should takes place using watchdog. The node which detect this, should forward this information to source node.

To isolate that node from communication, the source will broadcast this information to all over the network. After that it will send route request to find alternative path.

For example, let assume one sender with two receiver sender [11], receiver [21], receiver [33] respectively.11, 21, and 33 denotes node's position. Then we define routed path using topology formation. After that, packet will be transformed to node by node. Some nodes are forwards the packets to another node but few nodes are does not forward the packets to another node. It is called malicious node.

Graph Design Based Result

Finally the results are displayed in graph structure. Graph is an essential part of display a result, so we plot a graph to show a various result comparison with packets, throughput, energy efficient and etc.

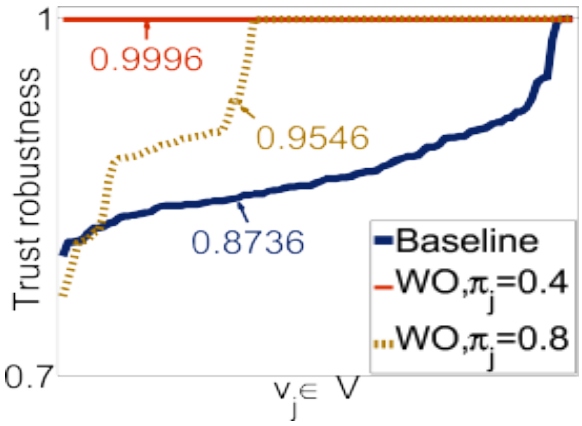


Fig 3: Trust robustness

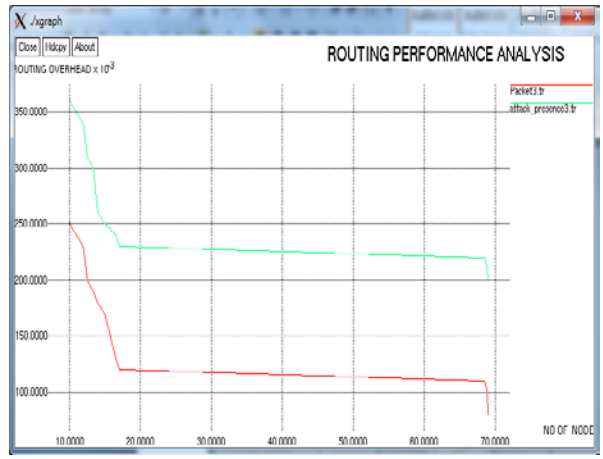


Fig 4: Routing overhead

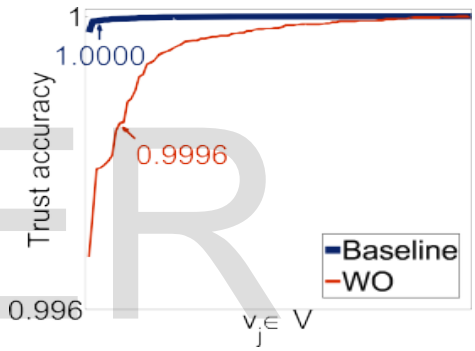
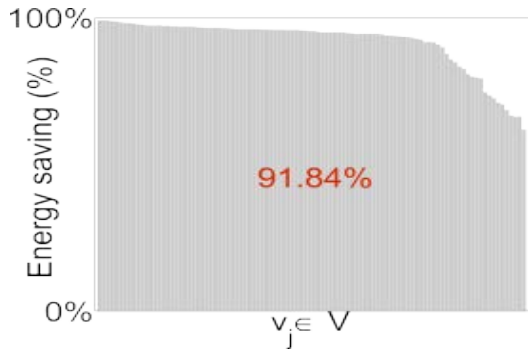


Fig 5: Trust accuracy



Existing approach to

Proposed approach

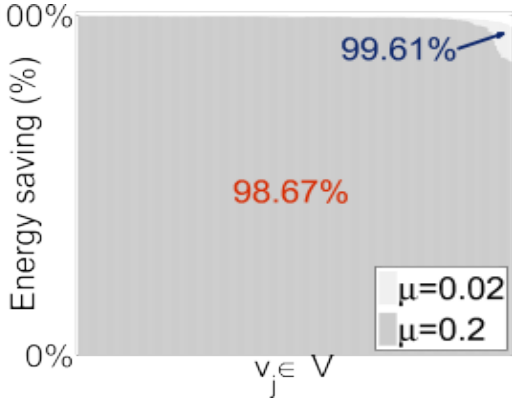


Fig 6: Energy saving

VII. CONCLUSION

The problem of selective jamming attacks_in wireless networks is addressed. An internal Adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets is considered. Jamming attacks on voice communications have been launched since the 1940s. In the context of digital communications, the jamming problem has been addressed under various threat models. The findings show that a selective jammer can significantly impact performance with very low effort. There are three schemes that are developed to transform a selective jammer to a random one by preventing real-time packet classification.

VIII. EFERENCES

[1] Shanshan Zheng and John S Baras. Trust-assisted anomaly detection and localization in wireless sensor networks. In Proc. Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011.

[2] Jonathan Tate, Benjamin Woolford-Lim, Iain Bate, and Xin Yao. Evolutionary and principled search strategies for sensornet protocol optimization. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 42(1):163–180, 2012.

[3] Roberto Di Pietro, Gabriele Oligeri, Claudio Soriente, and Gene Tsudik. United we stand: Intrusion resilience in mobile unattended wsns. IEEE Transactions on Mobile Computing, 12(7):1456–1468, 2013.

[4] Wendi B Heinzelman, Anantha P Chandrakasan, and Hari Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 1(4):660– 670, 2002.

[5] Riaz Ahmed Shaikh, Hassan Jameel, Brian J d'Auriol, Heejo Lee, Sungyoung Lee, and

Young-Jae Song. Group-based trust management scheme for clustered wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 20(11):1698–1712, 2009.

[6] Pietro Michiardi and Refik Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced Communications and Multimedia Security, pages 107–121. 2002.

[7] Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, and Ahmed Helmy. Location-centric isolation of misbehaviour and trust routing in energy-constrained sensor networks. In Proc. IEEE International Conference on Performance, Computing, and Communications, 2004.