INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue1)
Available online at: www.ijariit.com

An Improved Energy Aware Trust Derivation Scheme using Game Theoretic Approach

Abhijit M. Mandape
Communication Network
Dept.of E&TC, D. Y. Patil College of Engineering
Akurdi, Pune, India-44
abhijeet.mandape@gmail.com

Mrs. Sayali S. Mane
Assistant Professor
Dept. of E&TC, D.Y.Patil College of Engineering
Akurdi,Pune,India-44
sayali.mane@rediffmail.com

Abstract— In wireless sensor networks (WSN) trust plays a very important role, which is one of the most popular network technologies for the Internet of Things (IoT). The efficiency of the trust evaluation process is largely comprised by the trust derivation, as it influences the overhead in the process, and performance of WSNs is particularly sensitive to overhead due to the limited bandwidth and power. This paper extends the previous work of energy aware trust derivation scheme using game theoretic approach, by increasing the overall trust derivation process and improving the energy consumption which manages overhead while maintaining adequate security of WSNs. A risk strategy model is first demonstrated to stimulate WSN nodes cooperation. Then, a game theoretic approach with secure report reading and trust derivation algorithm is applied to improve the overhead of the process. We show with the help of simulations that our improvement in the overall trust derivation scheme can achieve both intended security and high efficiency suitable for WSN-based IoT networks.

Keywords—Energy Awareness, Game Theory, Internet of Things (IoT), Security, Trust Evaluation, Wireless Sensor Network (WSN).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are comprised of multiple sensors which are connected to each other in order to perform collaborative or cooperative functions. These nodes are typically connected as a multi-hop mesh network. WSNs are used in various applications such as environmental monitoring, health and medical monitoring, industrial monitoring, and many other applications. With the recent advancements in wireless communications sensor technology, and embedded system, we witness a exponential growth in the number of sensing devices connected to the Internet. The needs for mobility and convenience access also encourage the use of wireless for the Internet access. These recent developments have made wireless sensor network (WSN) one of the most important network technologies in Internet of Things (IoT). With these developments WSNs have become an attractive platform for many services. Despite the advancements in WSN development, there are still a number of problems that remain unsolved in WSNs.

Security is one of the primary challenges for the practical implementation of IoT. WSNs are many times deployed in remote environments which are venerable to attacks and hard to protect physically. Deployed sensor nodes may be harmed without knowledge, or malicious nodes may be introduced secretly into a WSN to compromise the security of the WSN. Furthermore, the sensor nodes that belong to different developers or service providers may not completely function with one another. For example, they may be configured for resource conservation which operates in a selfish manner. All of these can lead to degradation in performance or malfunctioning of WSNs.

Cryptographic techniques represent a practical method to deal with the security issues in many research fields. Unfortunately, their application to WSN-based IoT has been limited. Consequently, trust plays a crucial role in security techniques for WSNs. Trust of nodes is composed of direct 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 computation and 2) trust derivation. The former refers to the process of calculating the synthesis trust value based on the observed direct trust and collected indirect trust, whereas the latter represents

Since many trust models have been proposed in recent, most only focus on trust computation. As the accuracy of trust computation depends on the amount of recommendations received, the trust derivation process that provides how recommendations are passed on plays a crucial role. Given the power and bandwidth limitation in WSNs, the impact of recommendation circulation on the overall performance of WSNs is relatively high. Therefore, developing an efficient trust derivation scheme is part of a critical issue in the development of WSN-based IoT networks.

In this paper, we propose an energy-aware trust derivation scheme for WSNs, which cease to reduce the energy consumption of the network under the premise of security assurance. First, we provide a strategy analysis to stimulate the nodes' cooperation. By using this method, we derive the desired number of recommendations. Next, trust derivation dilemma game (TDDG) is introduced into the trust derivation process to reduce the overhead of the network. Finally, by conducting extensive simulations, we show that our approach can not only maintain the desirable security of the network, but also significantly reduce the energy consumption and latency of the network compare with traditional mechanisms.

II. RELATED WORKS

With the increase attention in the field of security for WSNs and IoT, there has been an increase in the development on trust evaluation in current years. In order to improve the precision and accuracy of trust computation, most trust models are focused on the trust computational process by using modeling tools and mathematical analysis, such as D-S theory and beta probability distribution model. However, as algorithms of trust computation do not contribute much to the overall operational overhead, these models will not have much effect on energy use. By contrast, the trust derivation is a process in which data interactions affects significantly to the energy consumption and latency of trust evaluation. This paper contributes to the trust derivation process.

In trust evaluation systems, an evaluating node or a source node that launches the trust derivation process should get all trust information from others for trust computation. Trust data may be obtained indirectly or directly. A source node may make direct observation on its neighbors to detect the trust information easily by say intrusion detection mechanisms such as watchdog and path rater. Determination of other nodes outside of its direct communication adds uncertainty and complexity to the process. Recommendation has been a common way to achieve indirect trust. Due to the need for interactions among nodes, and more interactions usually leads to more number of recommendation accuracy but more WSN resource consumption, there is a tradeoff between the efficient of WSNs and the accuracy of recommendations. In order to minimize the overhead of the network, and un weighted node evaluation scheme Node Evaluation with Assistant Trust (NEAT) is proposed to guide the central node with evaluating its neighboring nodes' trust. When the central node asks to evaluate a neighboring node's trust, it will ask its informants about this neighboring node. The informants will then provide the queried node's trust values in their individual communities to the central node. However, limited by the characteristics of intrusion detection mechanisms, most abnormal behaviors started by malicious nodes can only measured by their neighbors. In order to reduce the overhead, the informants are often fixed to the neighbors of the central node, and they are unable to guarantee the quality of being trusted and validity of recommendations. Focusing on trust dissemination process, Olivier and Romano propose a process that incorporates update of trust values into routing. In the proposal, trust information is enclosed in a route request packet which could make full use of 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 neighbors of the receiving node, it ignores the reputation information and leaves it unaffected in the forwarded route packet. Otherwise, it uses the reputation value in order to update the computed reputation value with its local observation. This new value is then inserted in the route request packet, and broadcast to all neighbors. The main problem of this approach is its insecurity. Any intermediate node that receives the route request packet in route discovery process can tamper the trust value, which can significantly affect the credibility of trust values. A trust-aware routing protocol (TARP) is proposed.

Two steps are used to find a trusted neighbor node.

1) 1st step is called the "One Hop Check and will only be started by the source node that has some data to send. The source node will send a Neighbor Request to all its neighbors asking them for their trust values. Once it gets the trust values, the source node will choose the most trusted node.

2) In step 2, the source node will make a check on the preselecting node by communicating 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, more neighbor nodes of pre selected node will receive the request and response with a distant neighbor reply. However, to implement this approach, frequency-hopping and synchronization technologies are needed. Broadcasting reputation is another method for receiving recommendations from neighbors. The source or the evaluating node broadcast the trust request that has the identity of the evaluated node. If a receiving node is a neighbor of the evaluated node, it will reply the corresponding trust information. Otherwise, it only forwards the trust request packets. As flooding is involved in the process, this approach may produce a high overhead and energy consumption due to the flooding process. Game

theory offers devices to model strategic interaction among rational beings. It is also helpful for WSNs to analyze the sensor nodes' cooperation behaviors. Zheng et al. quantitatively analyzed the efficiency of establishing trust for improving node cooperation by studying a graphical game. However, they do not consider the security requirements of the network. Kamhoua et al. present the interconnection between cooperation, trust, and security in the network. But they do not provide methods to reduce the overhead of the network which is produced by the security mechanisms. Further, these schemes only utilize the computed trust value for dealing with other issues; none of them focus on the trust evaluation process itself.

III. SYSTEM MODEL

A. Network Model

In this paper, we consider a WSN consisting a number of sensor nodes and a few sink nodes that are distributed randomly in a designated area. Each sensor node is in charge of both forwarding packets and detecting events. All the sensor nodes are resource-constrained and have the same limited radio coverage. As a result, end-to-end communication in a WSN is normally achieved via multichip relaying where a communication path is established in a distributed manner. Table I lists the main notations that are used in the remainder of this paper.

B. Security Model

With remote and open deployment environment, WSNs are generally vulnerable to various attacks, such as black hole attack, wormhole attack, and Sybil attack. In this paper, 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) active and 2) passive.

In passive attacks, malicious nodes may passively gather sensitive information or behave selfishly 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).

Table I Notations for TDDG

Symbol	Meaning
R_j	Quantifies the reputation of node j
$f_g(e_j)$	Energy saving for node j
γ	A parameter specifying the ratio of reputation loss to energy saving
R_{th}	Reputation tolerable threshold
V	The set collecting all nodes in network
l	Round number
$\Delta T_D(i,j)$	The overall direct trust value of node j for node i
$\Delta T_I(M,j)$	The overall indirect trust value of node j for node i
$P_j(a)$	Positive or well behaved activities
$N_j(a)$	Negative or misbehaved activities
ΔT_j	Changes of trust value
ΔE_j	The amount of energy saving
k	The optimal number of recommendations
N	The number of participating nodes
G	The Utility
p	The probability of sending trust reply
$f_s(e)$	The cost to an arbitrary node to send trust reply

C. *Trust Model*

Trust model essentially performs trust derivation, computation, and application 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 a 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 and networking: securing routing, access control, and key management.

IV. Analysis of Security Requirements for TDDG

WSNs are usually employed in an environment without any central infrastructures and vulnerable to attack. In this paper, we assume that distant sensor node is compromisable and may not cooperate with other nodes. As mentioned above, the distributed detection technologies and trust evaluation methods are proposed to ensure the security of the network in this case. The aim of this paper is to reduce energy consumption and latency for trust evaluation while maintaining adequate security. Before introducing TDDG, we first calculate the security issues and measure the demand for network security. Fig. 1 illustrates the trust derivation for an arbitrary node. In the figure, *j* node is the evaluated node *i* node is the evaluating node. In order to secure the network, we use a risk strategy model to stimulate the nodes for proper security behaviors. We begin by defining the following network risk condition:

$$R_j - \gamma f_g(e_j) \geq R_{th} \qquad (1)$$

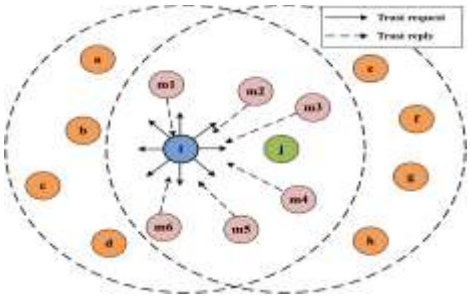

Fig. 1. Process of trust derivation.

Where R_j represents the reputation of node after some evaluation. The function $f_g(e_j)$ is the energy saving for node if it does not assist with a collection of proper behaviors. One example that a node may gain energy with misbehavior is a selfish behavior where the node does not forwards the data packets as it should according to the protocol specification. Such improper behavior has risk to the proper functioning of the network, and it should be avoided. The coefficient (e_j) is estimating the ratio of reputation loss to energy saving. Thus the left hand side of (1) determines the overall reputation of node after its potential misbehavior. We set a tolerable threshold R_{th} such that if the overall reputation remains aboveR_{th}, the proper network function involving node j can be maintained. Quantities R_j and R_{th} are normalized to give values between 0 and 1. Let V be the set collecting all nodes in the network, then (1) depicts the minimum condition for the whole network to function properly. From the nodes prospective, if it attempts any improper behavior, it will be valued by lowered reputation rating. At the point when its reputation rating is not sufficiently high, any attempt of improper behavior to conserve energy will violate the condition set in (1) with consequences of being evicted from the network. Thus, the condition also stimulates the proper behavior of nodes.

In the proposed model, reputation and risk are evaluated periodically. The instantaneous reputation of node *j*, which is also the overall trust value at round *l*, is defined as the difference between the positive and negative trust values combined from indirect and direct observations. It can be written as

$$R_j = \Delta T_j^{(l)} = f_t(\Delta T_D(i,j)^l, \Delta T_1(M_j,j)^{(l)}) \qquad (2)$$

Where $\Delta T_D(i,j)^l$ and $\Delta T_1(M_j,j)^{(l)}$ represent the overall indirect trust value and direct trust value of node *j* for node *i* at l^{th} round. The quantity M_j is the set of nodes providing recommendations of node *j* for node *i*. The function *f (.)* defines how direct and indirect trust values are brought together.

v. PROPOSED WORK

The proposed network consists of wireless sensor nodes distributed randomly in an entrusted environment. The nodes are aware of their location and include their address in each packet they transmit. As depicted in Figure 2, the blue nodes represent the destination and source nodes; the pink nodes are the neighboring nodes and the red node represents the attacker node the black circles represent the communication ranges of the victim and attacker nodes, respectively.

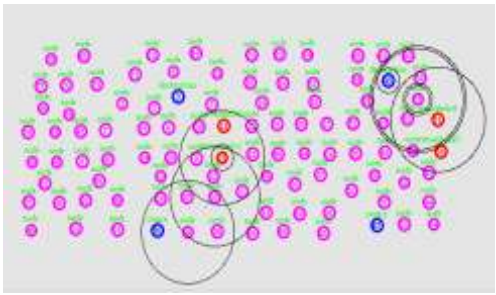

Fig. 2 Arrangement of WSN

For the transmission of the data packets between source and destination AODV routing protocol is implemented.

A wormhole attack is simulated between the source and destination. The wormhole attack consists in recording traffic from one region of the network and replaying it in a different region. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where A and B are not themselves within transmission range of each other. Intruder node X merely tunnels control traffic between A and B (and vice versa), without the modification presumed by the routing protocol. This results in non existence of A - B link which in fact is controlled by X, as shown in Figure 3.1. Node X can afterwards drop tunneled packets or break this link at will. Two intruder nodes X and X′, connected by a wireless or wired private medium, can also collude to create a longer (and more harmful) wormhole, as shown in Figure 3.2

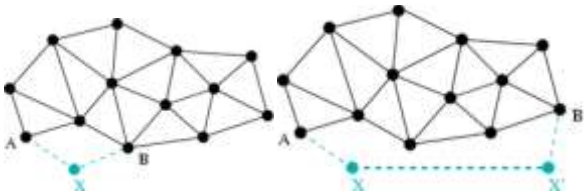

fig 3.1 fig 3.2

Figure 3.1: A wormhole created by node X

Figure 3.2: A longer wormhole created by two colluding nodes X and X′.

The following performance results were obtained. The graph 4.1 represents delay, the fig 4.2 represents throughput and fig 4.3 represents energy consumption in the presence of wormhole attack.

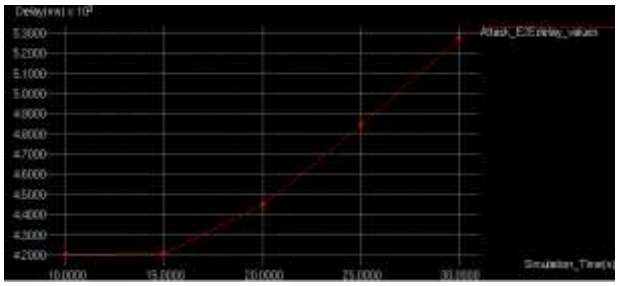

Fig 4.1 Delay Vs Simulation Time

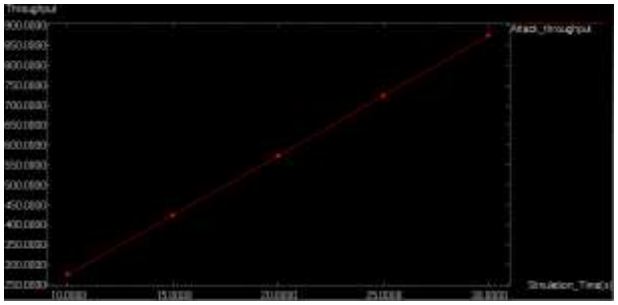

Fig 4.2 Throughput Vs Time

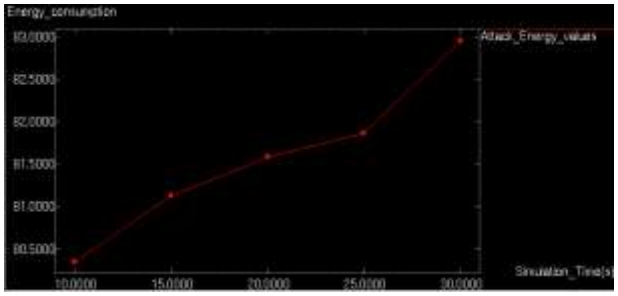

Fig 4.3 Energy Consumption Vs Time

Now Implementation of TDDG (trust derivation dilemma game) is done by using secure report reading and trust derivation algorithm in WSN and with more number of nodes to transmit the packets from source to destination and reduce energy consumption with low delay. The following results are obtained.

IV.RESULT

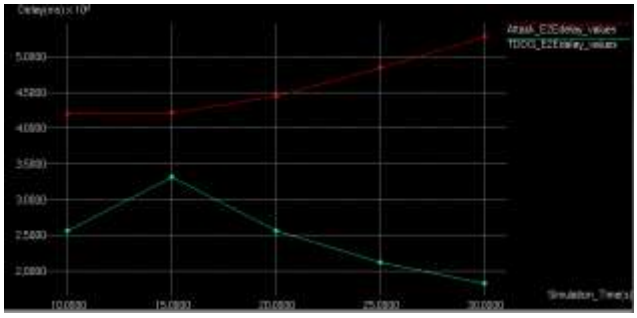

Fig 5.1 Delay VS Time

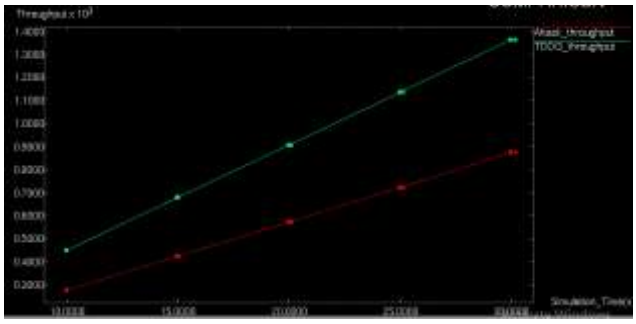

Fig 5.2 Throughput VS Time

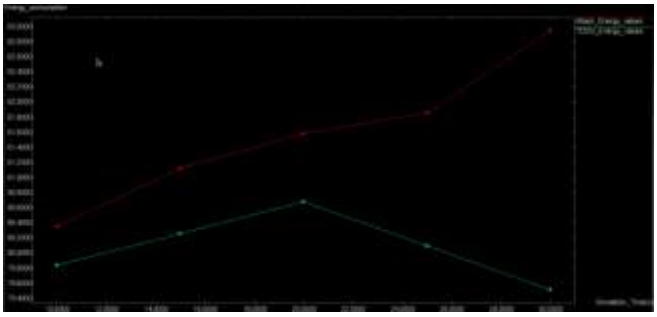

Fig 5.3 Energy Consumption VS Time

From the above three figures it can be seen that by the implementation of TDDG by using secure report reading and trust derivation algorithm the delay and energy consumption can be decreased with the increase in the throughput.

CONCLUSION

We proposed modified technique to enhance the estimation accuracy and energy consumption by implementation of TDDG (trust derivation dilemma game) by using secure report reading and trust derivation algorithm in WSN and with more number of nodes to transmit the packets from source to destination and reduce energy consumption with low delay. Compared the performance of attack with TDDG using measured parameters and it was found that the proposed enhancement improves the system performance.

In future we enhance this TDDG by using LISA (light weight security algorithm) concept and improve the performance of the network.

REFERENCES

1) Junqi Duan, Deyun Gao et.al "An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IOT Applications" IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014.
2) R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," Computer, vol. 44, no. 9, pp. 51–58, 2011.
3) P. Kasirajan, C. Larsen, and S. Jagannathan, "A new data aggregation scheme via adaptive compression for wireless sensor networks," ACM Trans. Sensor Netw., vol. 9, no. 1, pp. 1–5, 2012.
4) R. Zhang, J. Shi, Y. Zhang, and J. Sun, "Secure cooperative data storage and query processing in unattended tiered sensor networks," IEEE J. Sel. Areas Communication, vol. 30, no. 2, pp. 433–441, Feb. 2012.
5) Jian-Ming Chang et.al. , "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015.
6) G. Theodorakopoulos and J. Baras, "On trust models and trust Evaluation metrics for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2,
7) 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,
8) H. Xia, Z. Jia, X. Li, L. Ju, and E. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," Ad Hoc Netw., vol. 11, no. 7,pp. 2096–2114, Sep. 2013. status and achievements". Computers and Electrical Engineering, Vol.29,No.1, pp.25-44, January 200

