Trust Management in Wireless Sensor Networks: An Optimal Approach

Arul Treesa Mathew, Neena Alex
Department of Computer Science and Engineering
St. Joseph's College of Engineering and Technology Palai

Abstract— **Wireless Sensor Networks have gained popularity these days. They have a wide area of applications. Despite of this, WSNs are also prone to a number of threats. Trust Management Schemes have been found efficient in protecting the WSNs. Many ways have been proposed to build a trust management system for WSNs. Among them Game Theory based approaches are found to be efficient in handling a huge population. We propose a scheme where trust and privacy can move hand-in-hand.**

Index Terms— **WSNs, Trust Management Systems, Privacy**

I. INTRODUCTION

The wireless sensor networks had emerged as a revolutionary movement in the field of technology. Wireless sensor network- a collection of sensor nodes, each with its own sensor, connected via a wireless medium can provide an unique ability to examine the physical world accurately. Wireless Sensor Networks have found their application in various areas ranging from medical to military, and from home to industry. Despite of all these applications, they are highly prone to a wide variety of threats- both external and internal. The traditional security mechanisms of cryptography will not be sufficient to secure a Wireless Sensor Network from what is called a soft security threat. It refers to internal attacks which occur from within the network. The traditional techniques fail to detect selfish behavior from these nodes within the network because they surpass the cryptographic checks. To handle these kinds of threats, the Trust and Reputation Management Systems (TRM) came into existence.[1]

The main goal of the TRM systems is to reduce the impact of misbehaving or faulty nodes. Generally, misbehaving nodes can be categorized as: 1) selfish nodes, which seek to maximize their own gains at the expense of others; and 2) malicious nodes, which act to degrade the system or individual node performance with no explicit intention to maximize their own gains. [1]

Trust in WSNs is the credibility of a node with respect to another. **Reputation** is the credibility of a node with respect to a group of other nodes. **Trust** can be defined as the degree of belief about the future behavior of other entities, which is based on one's past experience with and observation of their actions. Survival of a WSN is highly dependent upon the cooperative and trusting nature of its nodes. TRM system can be used to determine how much credibility to give to each node during the collective decision making process.

Many models have been proposed, but proper care for privacy of data along with trust calculation has not been given yet. We propose a scheme where the privacy of data can be preserved along with the trust value computation.

II. LITERATURE REVIEW

We have performed a detailed study on wireless sensor networks, various attacks possible on them, different trust management schemes and their merits and demerits. The important ones are listed below.

The paper proposed by Yanli Yu et. al categorizes various attacks and their counter measures related to trust schemes in WSNs. WSNs are easily vulnerable to attacks which are either external or internal where External attacks: via eavesdropping or traffic analysis. No control over any particular nodes and Internal attacks: intruder breaks through any traditional safeguards to a node and learns crucial information from it. It is difficult to determine the type of attack a node suffers from, since the attacks have similar malicious behavior sometimes.[2]

In the paper, proposed by Haiguang Chen, the nodes are assumed to maintain reputation for other nodes of several different tasks and use it to evaluate their trustworthiness. They propose a task based trust framework for sensor networks (TTSN). Sensor node has different trust rating for different task while co-operating with other nodes. Collaboration between neighboring nodes is required in WSNs. Performance of nodes may vary with the tasks they attend. For very low trust ratings for a given task in a node, the neighboring node may stop cooperating with that node. A Task and Trust Manager Module runs on each node of the network and acts as the trust entity. 3 components for Task and Trust Manager Module include: The Monitoring Module which can classify different packet forwarding activities related to different tasks; if anomaly detected, it notifies the task and trust handling module, The Reputation Handling Module which gets different reputation output value for different tasks. It uses a task function to generate score of the performance and The Trust Handling Module in which trust is built using Bayesian formula [3].

The paper proposed by Azzedine Boukerche et al takes into consideration the power and bandwidth constraints of WSNs. It proposes localized trust and reputation management and storage strategy. The system has two phases of execution: Network Initialization phase where the agent gets attached to each node, ie a local agent for each node in the network and a Service offering phase where the actual service of trust management is offered by the attached agent. The advantage is that there is no need of flooding the network with request messages. The work is found to provide minimal overhead and can be adequately adopted for wireless sensor networks. [4]

ISSN: 2278 – 7798

The paper by Wen Shen et al proposes a novel energy prediction based scheme for trust management in sensor networks. The system prevents the election of compromised or malicious nodes as cluster heads. It introduces novel vice-head nodes to monitor the cluster heads' behaviors in case of their betrayal. The scheme is intended to protect against the denial of service (DoS) attacks. It detects DoS attacks when nodes are electing trusted clusters. It employs trust evaluation at different levels of cluster: Node level, Cluster head level and Base station level. It optimizes the cluster head election by electing vice cluster heads to find out the betrayal of elected cluster heads. It can be applied to defend against DoS attack by both detecting malicious nodes and preventing them to become cluster heads.[5]

The paper proposed by Shigen Shen et al [6] describes an evolutionary game theory based trust model for wireless sensor networks. Game theory can be used to analyze system operations in decentralized and self-organizing networks. It models situations where the decision makers may make specific actions having mutual – possibly conflicting – consequences. Game Theory describes the behavior of players in a game. Players may either cooperate or non-cooperate while trying to maximize their own outcomes from the game. In the case of wireless networks, game theory can be used as a tool for building cooperation schemes among entities such as nodes, terminals or network providers. Game theory performs scenarios where multiple players with contradictory objectives compete with each other; it can provide a mathematical method for analyzing and modeling WSNs Security problems. Therefore, it is very suitable to employ game theory to solve WSNs security issues. A game has three components: a set of players, a set of possible actions for each player and a set of strategies. A player's strategy can be defined as the complete action plan to be taken when the game is actually played. Players may act selfishly to maximize their gains and hence a distributed strategy for players can provide an optimized solution to the game.

Evolutionary game theory imagines that biologically conditioned players randomly drawn from a large population play the game repeatedly [6]. It is designed to enable an analysis of evolutionary selection in such precisely interactive environments. According to evolutionary game theory, individuals who act their strategies better will increase their rates in the population, while those who act worse will decrease. In a wireless sensor network, sensor nodes are considered individuals and WSNs as the population. Evolutionarily stable strategies are explored to demonstrate the stability of WSNs. The goal is to find out the evolutionarily stable strategies of the network by repeating the game to several numbers of rounds. This result will help in designing a good trust management system for the network. The trust management system is good if the evolutionarily stable strategy achieved is almost always that which maximizes trust.

The trust game for sensor nodes consists of a 4-tuple **G (P, N, S, U)**, where:

- **P** is a population composed of a large no. of individuals (sensor nodes in case of WSNs)
- **N** is the set of individuals in the same population P
- **S** is the set of strategies, and **S = {S1, S2}**
  S= {Trust, Distrust}
- **U** is the payoff matrix

Trust level is generally used to measure the trust relations among sensor nodes. In the trust game, each sensor node may select the strategy Trust or Distrust. Selection of Trust strategy by a sensor node means that it will cooperate with its counterpart; on the other hand, selecting Distrust means noncooperation. The authors examine various cases and their associated payoffs.

Trust relationships among sensor nodes can help to build their confidence to cooperate with others and reduce the risk of cooperation. The trust game for sensor nodes that is described in the paper can reflect sensor nodes' utilities during their decisions of selecting the strategy Trust or Distrust. The evolutionarily stable strategy is explored for each node thus analyzing the whole network.

Afrand et al. based on cooperative game theory proposed a game between a sensor node and three factors - cooperation, reputation and quality of security. Cooperation between nodes means there is more reliable data communication between nodes and moreover when a node cooperates its reputation increases and misbehavior is easily detected. By combining these factors the trust value is calculated [8].

Dai Hongjun el al proposed a method which uses a novel entropy based model and evaluation methods to find trust. First entropy based trust calculation model is found to get the trustworthiness between two nodes. Then to get the trust value of one node to another using direct action, a probability action [0,1] is followed. In the third step the trust is established between nodes using recommendations and directed graph is used to describe the trust values [9].

Zahra et al. proposed an energy efficient trust based algorithm which concentrates on aggregation and energy. The concepts of functional reputation and trust are used to select nodes that best satisfy the criteria to be an aggregator on the basics of quality of the node. In order to find best path from every sensor node the link availability and residual energy of nodes are taken into account. The disadvantage is that it introduces some delays in the network but overall it outperforms in terms of reliability and lifetime (Energy) [10].

Wenbo He et al. proposed an effective scheme for preserving privacy as well as for aggregating data in WSNs. In this paper, two privacy-preserving data aggregation schemes for additive aggregation functions are proposed. The first scheme – *Cluster-based Private Data Aggregation (CPDA)*–uses clustering protocol and algebraic properties of polynomials. It has the advantage of causing less communication overhead. The second scheme– *Slice-Mix-AggRegaTe (SMART)*–works on slicing techniques and the associative property of addition. It has the advantage of causing less computation overhead. The paper aims to bridge the gap between collaborative data collection by wireless sensor networks and data privacy. [11]

III. PROPOSED SYSTEM

We propose a system which uses Evolutionary Game Theory to find out the trust strategies of a node to another in a WSN and then employs privacy to the data being transferred between the nodes that are found trustworthy.

The evaluation of trust is between two nodes in the same network at a time. It will then be extended to the network. Each node will first prepare their initial strategy of trust/distrust the other node. This is done by evaluating the trust values derived in the initial examination. Two factors

affect the derived trust value- direct trust or the trust the node has rated to the other node based on its past experience and neighbor trust or the trust rating, a node can decide to the other node based in the recommendations from its neighbors. The direct trust and neighbor trust values will be passed through the exchange of HELLO messages. The protocol we have opted is an extended version of the AODV protocol.

The initial value is derived as a function of both the direct trust and neighbor trust values. This trust rate will be analyzed and then compared with a predefined threshold value. This will lead to choosing an initial trust strategy i.e. whether to trust or distrust the other node initially.

The phase following this is the evolutionary game. As the name indicates, using this game we try to build the evolutionarily stable strategy of the node to the other. The nodes constantly try to adjust their strategies towards each other. While repeating the game for a several no of times, the evolutionarily stable strategy of the node to the other will be evolved. This derived strategy is analyzed.

The nodes are allowed to communicate if and only if the evolved strategy is trust.

The privacy of data will be the new concern. The data to be transmitted will be first forwarded to randomly selected neighbors of the source node after securing it and then from these neighbors the received data will be passed to the query server in the Base Station after providing a second stage of security. The base station is assumed to be the most trustworthy node of the network. The query server of the base station will then forward this data to the intended recipient. Since multiple nodes are involved in sending the data, the source location privacy is preserve and also the use of security techniques preserve the data content privacy.

IV. CONCLUSION

The game based trust management system being used here is found to be effective since game theory is found highly efficient in deriving a decision from a huge population. Since the final strategy is derived after an evolutionary game, it is normally stable. The trust value computed initially uses both direct trust and neighbor trust values (i.e. both trust and reputation is analyzed here). The source location privacy and data content privacy has been protected here. The protocol used has been found efficient with minute variations in performance compared to AODV.

V. PERFORMANCE EVALUATION

PROTOCOL NAME	THROUG - HPUT	END TO END DELAY	PACKET DELIVERY FACTOR
AODV	**420.10 kbps**	**207.746 ms**	**0.9788**
TRUST BASED PROTOCOL	**407.66 kbps**	**217.837 ms**	**0.9835**

VI. FUTURE WORKS

The system analyses the trust between two nodes only. The next phase of our work is to build a trust management system which can analyze all nodes in a network together. The privacy scheme for data transmission will also be concentrating on partitioning and then aggregating data throughout the transmission.

REFERENCES

[1] Arul Treesa Mathew, Neena Alex "A Study on Game Theory Based Trust Decisions", *RACIE 2014*

[2] Yanli Yu et. al. "Trust mechanisms in wireless sensor networks: Attack analysis and Countermeasures*", Journal of Network and Computer Applications 35 (2012) 867–880*

[3] Haiguang Chen, "Task-based Trust Management for Wireless Sensor Networks" *International Journal of Security and Its Applications Vol. 3, No. 2, April, 2009*

[4] Azzedine Boukerche et al, "An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks", *IEEE Globecom 2005*

[5] Wen Shen et al. "Energy Prediction based Trust Management in Hierarchical Sensor Networks", *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*

[6] Shigen Shen et al, "Evolutionary Game Based Dynamics of Trust Decision in WSNs", *2013 International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)*

[7] Hai-Yan Shi, Wan-Liang Wang, Ngai-Ming Kwok and Sheng-Yong Chen, "Game Theory for Wireless Sensor Networks: A Survey", *Sensors* ***2012****, 12, 9055-9097; doi:10.3390/s120709055, ISSN 1424-8220*

[8] Afrand et al."A game theory based approach for security in wsn", *IEEE International conference on Performance ,Computing and communication 2005 p 259-263*

[9] Dai Hongjun "An entropy based trust modeling and evaluation for Wireless sensor networks" *International conference on Embedded Software systems* ,ICESS 2008

[10] Zahra Taghikkaki "Energy efficient Trust based Aggregation in WSN " *INFOCOM WKSHPS '2011* 2011 p 584-589

[11] Wenbo He et al. "PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks"

ISSN: 2278 – 7798