Dynamic Trust Management for Non-Selfishness and Service Allocation Using Game Theory

B. Nandhini[1], Mrs. M. Praveena
M.Phil Scholar[1], MCA., M.Phil. Assistant Professor[2]
Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India

***Abstract*- Service Oriented MANET (SOMANET) is one of the most promising technologies that have applications ranging from Tele-service to other data services. There are several techniques proposed in literature to thwart intruders in SOMANET environment, Game theory is the most popular techniques used against service oriented attacks and intrusion problem. This study implements an optimal game theory to Service Oriented MANET (SOMANETs) against service oriented attacks. In order to manage SOMANETs with secure features, the proposed system creates a novel game theory driven approach named as TRAP, and that will be applied into the proposed protocol for service oriented architecture named as Dual Trust based service allocation protocol (DTSA). The main process of the proposal is the detection and prevention of attackers using game theory. This study proposes a new pattern for intrusion detection in SOMANET using fusion based paradigms, which are adaptive low interaction honeypots and game theory concepts. This approach performs the interaction between the game theory and honeypot. This effectively applies the production honeypot technique along with the new game theory approach such as strong Nash equilibrium here the game theory is a non cooperative game theory concept.**

***Keywords*- MANET, SOMANET, Game Theory, Honeypot, service attacks, Trust Management**

I INTRODUCTION

A Service Oriented MANET (SOMANET) is consolidated with network service providers and service requestors. This kind of network doesn't like to have malicious nodes which may collude to maximize their own gain and even monopoly service. Ad-hoc networks are the decentralized type of wireless networks that work without the help of a centralized control and with the features such as openness, distributed communication, self-configuration, self-organization, and limited bandwidth wireless channels. [1] In this process, nodes act as the router to identify the path, and as the host to generate the data and control packets. Therefore, in ad-hoc networks, [2] node cooperation is a vital factor for executing the protocol instructions.

1.1 Trust in MANET

Trust in MANET is the analysis of node in terms of "firm faith in the reliability, truth, or ability of someone or something". It is the degree of belief about the behavior of a particular node. In MANETs, due to high mobility, malicious nodes may frequently join and leave the network. [3] Trust is a dynamic one, which is not same always. The positive behavior can increase the trust and negative case decreases. Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. Trust reflects expectations on the honesty, integrity, ability, availability and quality of service. It also reflects the mutual relationships where a given node behaves in a trustworthy manner and maintains reliable communications only with nodes which are highly trusted. In MANETs, an untrustworthy node can cause considerable damage and adversely affect the quality and reliability of data.

1.2 Selfish Nodes in SOMANET

Node misbehavior due to selfish or malicious reasons or faulty nodes can significantly reduce the performance of SOMANETs. Node misbehavior means deviation from the original routing and forwarding. The source node can relay packets to the destination node through other nodes in SOMANET. [4] The selfish node does not participate in routing process, which intentionally delay and dropping the packet. These misbehaviors of the selfish nodes will impact the efficiency, reliability and fairness. A selfish node does not perform the process related to packet forwarding function for data packets unrelated to it. The selfish node utilizes its limited resources only for its own purpose because the energy and storage constraints for each node in the SOMANET. It aims to save its resources to the maximum, so this type of misbehaving node discards all incoming packets except those which are destined to it. The selfish nodes neglect to share their resources, such as battery power, CPU time and memory space to other nodes in SOMANET. This behavior is observed in the data link/MAC layer, which is decisive, specifically when the mobile nodes possess small residual power.

II PROBLEM DEFINITION

In the literature, Trust Based Heuristic Algorithm [5] with auctioning and local knowledge was used. Trust-based allocation protocols [6] were used to calculate the trust model in the existing system. Some of the techniques [7] [8] have introduced to solve the task assignment MOO problems. The major problems of existing solutions are described below.

1) The existing system was not considering the existence of malicious nodes acting for their own interest and colluding for individual welfare, and

2) Solving the task assignment MOO problem in exponential time complexity, making it unsuitable for runtime deployment.

Another main problem of SOMANETs is resource constraint, [9] where SOMANETs cannot pay for monitoring and analysis of the network traffic for anomaly detection every time. Anomaly or intrusion detection using game theory is a challenging task due to the dynamic nature of wireless nodes and its behavior. Several approaches could prevent the network from intruders, even though the system have created many false alarms and some techniques need to be adopted with existing component based IDS. So the communication and computational overhead increased. The system should work with Gaussian model for optimal intrusion detection. And only few researches concentrated on multiple attacks in ID. SOMANETs should detect anomaly or other malicious activities by means of single or two players.

III PROPOSED SYSTEM

The proposed research aim to develop complete security architecture for the service oriented MANETs, which have affected by different types of trust related attacks such as bad mouthing attack, ballot stuffing attacks etc. In SOMANET, there is a course to acquire methods for detecting different attacks and private access by an attacker against the stability of SOMANET, by using game theory based trust calculation schemes. In literature there are few exploration has been done in the development of optimal game theory in SOMANET for misuse and misbehave detection. This paper implemented an optimal game theory to Service Oriented MANET (SOMANETs) against intruders and selfish attackers.

3.1 Contributions of the proposed system

The contribution of this study consists of a game theoretic framework against Intruders over SOMANET. Here the intruders are represented as selfish attacker, interrupter and making service delays. This proposes and analyzes an interactive learning game model driven from game theory mechanism. This influences the equilibrium solutions for the proposed model and analyzes the resultant strategies of the attacker and the defender. This also proposes the use of chronological behavior of mobile nodes to reduce the communication overhead. This also performs trust based service allocation system in SOMANET to reduce and schedule the resource utility issues. So this is a strong Nash equilibrium solution which falls under a non-cooperative game theory.

IV DTSA

In DTSA framework intrusion detection is looked at in the form of a non-cooperative nonzero-sum game without have the interaction between mobile nodes. Here the players are the intrusion detection system (IDS) of the SOMANET which is named as DTSA and the attacker. DTSA appeals attackers by providing some false or fake information at the time of detection. DTSA require very less resources to run, therefore they are easy to use. Through DTSA events and activities of the attacker on the network are captured. In this study the interaction between an attacker and the defender system as a basic signaling game which falls under the dynamic non-cooperative game with incomplete information. In DTSA model of the dynamic game, a mobile node is the sender and the CH (Cluster Head) attached with IDS is the receiver to which the data is transmitted. The mobile nodes private information is identified as their sensed data. The mobile node divided into two types: the node could be a regular node or that could be an intruder or attacker.

4.1 Strong Nash Equilibrium

A statistics i.e. a Gaussian driven method has been applied in the strong Nash equilibrium,

The game being played each period

- A_p the action of player P taken in period T
- $A_T = (a_1^t, \ldots, a_n^t)$ the list of what each player played at E
- The whole log, where every period up to the present is defined as P_h
- $h^t = (a^1, \ldots, a^t)$ the list of what happened in each of the first t periods
- H^t the set of all possible histories of length T.
- $H = \mathbf{U}_t H^T$ the set of all possible finite histories.
- $S_i : H \rightarrow (A_{i\Delta})$ a strategy of i
- $S_i (h^t)$ specifies what i will do after a history h^t

So, $S_i (h^t)$ is a choice of a play in period t+1 after observing what happened in all previous periods chronologically.

4.2 Trust Calculation in DTSA

The trustworthiness of a node is evaluated based on their self-behavior. This will be used the game theory results and the honey pot records to evaluate the trust of every node. The basic idea is to build a trust model that provides with a mechanism to evaluate the trust of its neighbors. The proposed trust scheme contains a powerful tool for the detection of unexpected node behaviors. Once the selfish nodes are detected, their neighbors can use this information to avoid cooperating with them, either for data forwarding, data aggregation or any other cooperative function.

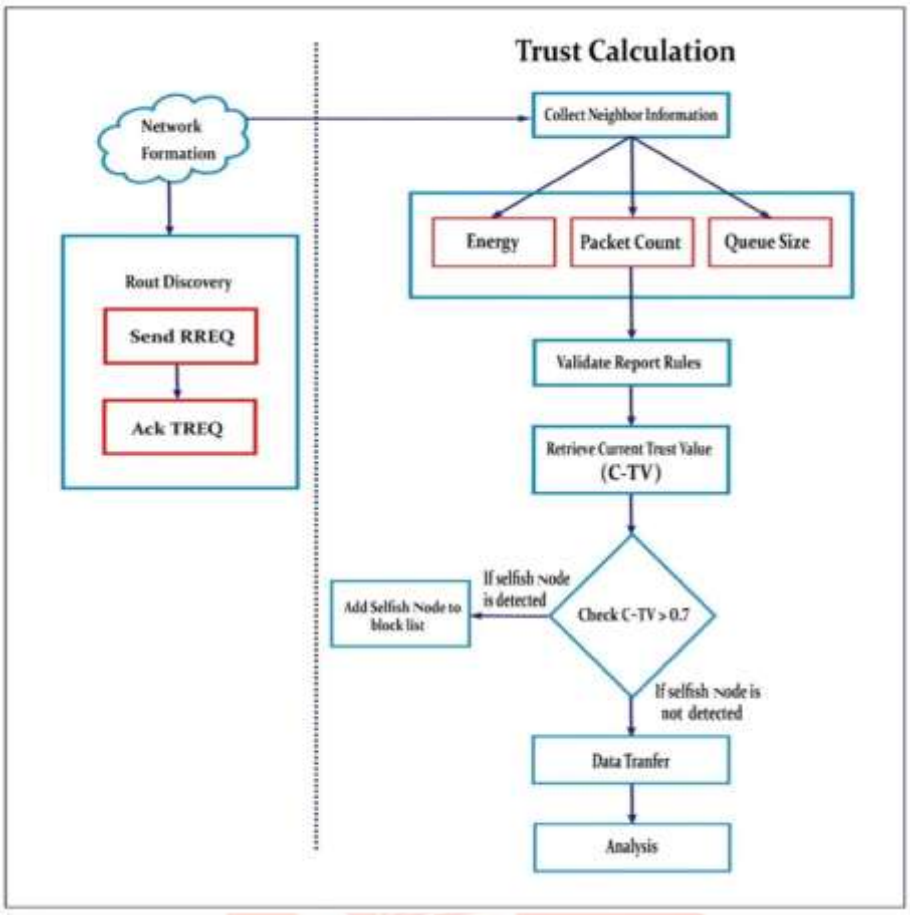

Fig 1: Overall Flow of the Proposed Record- and Trust-Based Detection (RTBD) Technique

4.3 Selfish Node Detection

All the nodes in SOMANET perform the routing function as mandatory and forward traffic, which other nodes had sent to it. Among all the nodes, some of the nodes behave selfishly; these types of nodes are called selfish nodes. Any node in SOMANET may act selfishly, which means using its limited resources only for its own profit, since each node in a network has the resource constraints such as storage and battery limitations. The behaviors of the selfish nodes are shown below:

Do not forward RREQ messages: This type of nodes does not forward the RREQ messages in SOMANET. It drops these packets to avoid being the route member for others.

Do not forward data messages: These kind of selfish nodes will forward the messages, but it does not rely on data messages and drop them. This misbehavior will impact the performance of SOMANET.

Delayed forwarding RREQ messages: These kind of selfish nodes forward the messages with a delay near the upper limit of timeout.

Do not forward RREP messages: If this kind of selfish node exists in SOMANET, it will drop all RREP messages received by these nodes.

4.4 Record-And Trust-Based Detection (RTBD) Technique with the DTSA:

In this framework, every node maintains a global trust state for all selfishly behaving nodes in the network. The trust state is maintained in the form of a trust table. A trust table contains two fields, namely *n-id* (*node id*) and *t-val* (*trust value*). When a node receives a new trust certificate, the trust state of a node is updated. The certificate is evaluated by verifying the response from every neighbor in the group. The impact of trust certificate in the final trust value of a suspected node depends on the trust state of the node.

Algorithm 1: Record –and –Trust Based Detection (RTBD)

//Route Discovery

Step 1 : Source *(S)* sends a RREQ to Destination *(D)*.

Step 2 : Destination *(D)* receives the RREQ from Source *(S)* and sends RRES to Source *(S)*.

//Trust Calculation

Step 3 : Neighbor information is gathered and sensed,

i. Energy.

ii. Packet Count.

iii. Queue Size.

Step 4 : It generates a report and validate the report rules.

Step 5 : The trust value is calculated using following equation,

$$T_c^{ij} = \frac{t_s + p/2}{t+p} \quad ts, t \geq 0, p > 0 \qquad (4.5)$$

where, *Tc* is the trust calculation, *ij* represents the node *i to j*, *D* represents direct trust, *ts* illustrates the time success, *t* is the time transactions and *p* is the positive real number.

Step 6 : The current trust value (C_TV) is retrieved.

```
if (C-TV > 0.6)
{
if (selfish node is detected)
Add selfish node to Block List (BL);
else
Transfer the data to destination node;
}
```

Step 7 : Finally, the performance is evaluated.

V IMPLEMENTATION

The system simulates the proposed model using NS2. To evaluate the performance of the techniques, the system has developed a NS2-based simulation environment. The set of simulation parameters and their value ranges are listed in below Table.

This evaluates the proposed scheme with the collaborative equilibrium for effective and secure node verification for intrusion detection in SOMANET environment. This defines that the system operates periodically in a time-slotted mode. The proposed system uses 50 mobile nodes with wireless channel.

This has been generated by the random moving model to predict radio propagation inside a building and consider random topologies with a total of 50 nodes.

5.1 Results

The first set of experiments is to compare the performance of different combinations of existing game theory schemes, node verification strategies. All strategies are tested under different request patterns: Attack Detection Ratio, average packet dropping, false positive rate, intrusion detection accuracy and verification delay.

VI CONCLUSION

The misbehavior of selfish nodes is a major problem in SOMANET. The selfish nodes do not participate in the routing process, which intentionally interrupts and make delay and dropping the packet. Additionally the system proposes a new technique, namely, Trust-and Record- Based Detection (RTBD) to detect the selfish nodes in an efficient manner using the honeypot. The suggested RTBD method is an effective method, which enhances the performance of MANET. This is also associated with the trust calculation process by the RTBD module by DTSA. In a non-cooperative game with incomplete information these model situations in which some players have some private information before the beginning of a game. As future work, the system leaves the co-operative game theory framework with honey-trap for further implementation. The system can also include other type of intrusion detection schemes rather than game theory.

REFERENCE:

[1] Natchetoi, Yuri, Huaigu Wu, and Yi Zheng. Service-oriented mobile applications for adhoc networks. In Services Computing, 2008. SCC'08. IEEE International Conference on, vol. 2, pp. 405-412. IEEE, 2008.
[2] Ververidis, Christopher N., and George C. Polyzos. Service discovery for mobile ad hoc networks: a survey of issues and techniques. IEEE Communications Surveys & Tutorials 10, no. 3 (2008).
[3] Wu, Bing, Jianmin Chen, Jie Wu, and Mihaela Cardei. A survey of attacks and countermeasures in mobile ad hoc networks. Wireless network security (2007): 103-135.
[4] Kargl, Frank, Andreas Klenk, Stefan Schlott, and Michael Weber. Advanced detection of selfish or malicious nodes in ad hoc networks. In ESAS, pp. 152-165. 2004.
[5] Wang, Yating, Ray Chen, Jin-Hee Cho, and Jeffrey JP Tsai. Trust-Based Task Assignment with Multiobjective Optimization in Service-Oriented Ad Hoc Networks. IEEE Transactions on Network and Service Management 14, no. 1 (2017): 217-232.
[6] Pirzada, Asad Amir, Chris McDonald, and Amitava Datta. Performance comparison of trust-based reactive routing protocols. IEEE transactions on Mobile computing 5, no. 6 (2006): 695-710.
[7] J.H. Cho, A. Swami, and I.R. Chen, Modeling and Analysis of Trust Management for Cognitive Mission-Driven Group Communication Systems in Mobile Ad Hoc Networks, in Int. Conf. Computational Science and Engineering, 2009, pp. 641-650.
[8] J.H. Cho, A. Swami, and I.R. Chen, Modeling and Analysis of Trust Management with Trust Chain Optimization in Mobile Ad hoc Networks, Journal of Network and Computer Applications, vol. 35, no. 3, 2012, pp. 1001-1012.

[9] Shah, Rutuja, Sumathy Subramaniam, Lekala Dasarathan, and Dhinesh Babu. Mitigating Malicious Attacks Using Trust Based Secure-Before Routing Strategy in Mobile Ad Hoc Networks. CIT. Journal of Computing and Information Technology 24, no. 3 (2016): 237- 252.
[10] Nandhini, B. Trust-Based Task Assignment with Multi-Objective Optimization in Service-Oriented Ad Hoc Networks-A Survey. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 6, (2017): 12275- 12280
[11] Sarvesh, V.; Gunes, E. On a Local Heuristic for a Reverse Multicast Forwarding Game. In *Proceedings of 2009 First International Conference on Networks & Communications*, Chennai, India, 27–29 December 2009.