DUAL TRUST BASED SERVICE ALLOCATION PROTOCOL FOR SERVICE ORIENTED MANET

B. Nandhini
M.Phil Scholar, Department of Computer Science,
Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India

M. Praveena
Asst.Professor, Department of Computer Science,
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. Due to the flexible nature of SOMANET, it suffers from various security and interruptions. To overcome those security issues in SOMANET, an optimal game theory is proposed. In order to manage SOMANETs with secure features, the proposed system creates a novel game theory driven approach for service oriented architecture named as Dual Trust based service allocation protocol (DTSA). In specific, DTSA prevents SOMANET from service oriented attacks like selfish attack and unauthenticated behavior. And this has been implemented in Service Oriented MANET. The main process of the proposal is the detection and prevention of misbehaves in the service process using game theory. This study developed a new pattern for misbehave 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 mechanisms along with the strong Nash equilibrium; here the game theory is a non-cooperative game theory concept. The DTSA scheme experimented using the NS-2 simulator and this pinned with existing mobile features. Finally the experimental result shows the performance improvement in terms of false alarm reduction, control communication overhead and accuracy.

Keywords: MANET, SOMANET, Game Theory, Honeypot, service attacks, Trust Management

http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=8&IType=12
1. INTRODUCTION

Service Oriented Mobile Adhoc Network is a migration of traditional mobile ad hoc networks, which provides the services to the mobile nodes. These service oriented architecture interacts with the nodes, receives their request and provides the necessary services to them [1]. As like the traditional MANET, SOMANET is deeply affected by several security and performance challenges [2] including dynamic topological changes, lack of battery and resources, unreliable communications and presence of misbehaving and malicious nodes. These issues may degrade the performance of the network, so this is necessary to develop a complete security solution for the service oriented networks. This paper concentrates on trust management and its applications for service-oriented MANETs to handle the above challenges which additionally include no centralized authority, dynamically changing topology, limited bandwidth and battery power, limited observations, unreliable communication, and the presence of malicious nodes who act to break the system functionality as well as selfish nodes [3] who act to maximize their own gain. The security of the SOMANET is becoming a vital issue. There are various techniques available for the security in MANETs. Based on the definition, this represents the trust model using game theory, which is used to formulate the trust between two nodes in SOMANETs and present a new prototype to achieve the same.

Data security and optimal service allocation in SOMANET will be a beneficial process to handle the trust issues. The proposed dual trust method is capable for the normal MANET scenario and as well as Service oriented MANET process. The current proposal is developed as a prototype, which can be enhanced for any type of network services and deployment can be performed for the different attack detections. The capacity of the attack detection scenario is higher in the proposed system, so the technique is suitable for high dense mobile networks. The deployment cost may not vary if the proposed system implemented in the multiple service architecture. With the use of honeypot and game theory ideas, the customized attack detection is performed and evaluated with various parameters.

1.1 Selfish Nodes In Somanet

Each mobile node in SOMANET requires the help of other nodes to forward the packets. The nodes are expected to wait for a pre-defined time interval between successive transmissions. But, a mobile node may misbehave due to network congestion and selfishness. In case of node misbehavior in the MANET or any malicious behavior occurred in the nodes, and then it can drastically decrease the performance of SOMANETs [4]. 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. The selfish node in the network will not be a part of network transactions and it sometime make delay or interrupts the transaction. 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. The main target of the proposed system is to save the node resources up to the maximum range. This eliminates the misbehaving node and its. 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. The features of the selfish nodes are,

- Non-participation in routing.
- No transmission or reply to HELLO messages.
2. PROBLEM DEFINITION:

Misbehave and selfish behavior detection is a challenging task due to the dynamic nature of wireless nodes and its unique behaviors. Several approaches have proposed to prevent the network from malicious users and interruptions, even though the system have created many false alarms and some techniques need to be adopted with existing network security components. This integration increased the communication and computational overhead. 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.

Recently authors in [9] developed trust-based solutions to mitigate these problems. In particular, a trust-based algorithm to solve the task assignment MOO problem in polynomial time complexity is proposed to making it possible to perform dynamic node-to-task assignment at runtime. Non-trust-based counterparts using blacklisting techniques have also developed to handle the trust issues in the SOMANET. Another main problem of SOMANETs is resource constraint, where SOMANETs cannot pay for monitoring and analysis of the network traffic for misbehave detection every time. And only few researches concentrated on multiple attacks in the SOMANET. SOMANETs should detect anomaly or other malicious activities by means of single or two players.

3. PROPOSED SYSTEM

Trust calculation and optimal service discovery can improve the network service performance. However, acquiring the trust values and the node behaviors to update the trust score is difficult when the nodes are dynamic in nature. 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 [10]. 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. In specific, the study of service oriented attacks and unauthenticated behavior with the trust based solution has been implemented in SOMANET. The main process of the proposal is the detection and prevention of selfish attacks and other service oriented attackers using game theory. The last objective is the performance evaluation of the proposed scheme using the NS-2 simulator and this pinned with existing mobile features, and a set of performance metrics such as: false alarm reduction, control communication overhead and improvement in accuracy along with other QOS metrics.

In this study a new pattern for selfish node detection in SOMANET is proposed using fusion based paradigms, which are adaptive low interaction honeypots and game theory
concepts. This performed the interaction between the nodes and verifies the node trust. This effectively applies the production honeypot technique along with the new game theory approach; here the game theory is a non cooperative game theory concept. This analyzed numerous existing game theory models and uses a new game theoretical model optimal for SOMANET, where the new approach analyzes the past behaviors and performs iterative learning from the log.

3.1 Advantages:
- The proposed method expands the security of SOMANET and also reduces the cost caused by IDS and monitoring mobile nodes.
- The method also considers the detection of selfish nodes in the network.
- Improves the accuracy and reduces the false alarm.
- With the use of new chronological data, the behavior of intruder can be easily identified.
- Detection of multiple attacks
- Energy efficient framework
- Reducing false alarm
- Tracking of attackers and broadcasting the attacker details
- Robust and optimal

3.2 Contributions:
The contribution of this study consists of a game theoretic framework against Intruders over SOMANET. Here the intruders are represented as a node, which performs selfish behavior, interrupter and making service delays. Using an interactive learning game model driven from game theory mechanism, the attacker is detected. With the influences of the equilibrium solutions the proposed model analyzes the resultant strategies of the attacker and defends the service attack. 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.
- A new scheme named as TRAP, which is a honeypot technique driven game theory with interactive learning mechanism is proposed.
- A Dual trust based service allocation (DTSA) with the strong Nash equilibrium is proposed.
- A new game theory with the fusion mechanism which is named as DTSA which is an extension of stochastic game model is developed.
- This also finds the selfish node in the network and calculates the trust score for every node.
- The proposed scheme has the ability to find flooding, spoofing attacks in SOMANET using the DTSA strategies.

4. DTSA:
Honeypot are used to monitor the attacker’s and the selfish behavior. It is an information system that allows the intruders to interact with it. The value of DTSA lies in unauthorized use of that resource which finds the intruder in SOMANET. 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. This will be helpful in learning new malicious activities, methods
and evidence can be collected against an attack for legal use and network security. The existing game formulation is rather unproductive. The DTSA increases the complexity of attacking choice over SOMANET. The DTSA defends attacks in almost all clusters at a time. In the honeypot framework in DTSA each node and cluster will have to act independently of the others. This DTSA limits the playing strategy which has decided by the ID. The current framework facilitates the intrusion prevention, detection and response schemes in a quicker way. For effective prevention the DTSA provides different strategies and for detection DTSA provides strong Nash equilibrium and finally for response, the DTSA provides effective payoffs and honeypot techniques.

4.1. 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 honeypot 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. The main intent of this process is to handle and detect selfish nodes in SOMANET using DTSA. In this work, the trustworthiness of a node is evaluated based on their behavior. The basic idea is to build a trust model that provides 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.

4.2. Route Discovery:

Route discovery allows any node in a SOMANET to dynamically discover a route to any node in SOMANET. The initial step of route discovery is to create the number of nodes with the indicated position. By sending the RREQ packet the route will be discovered between the source node and the destination node. A node initiating a route discovery broadcasts a Route REQuest (RREQ) message, which may be received by those nodes within wireless transmission range. If the route discovery is successful the initiating node receives a route reply message listing a sequence of network hops. The algorithm for processing RREQ and RREP messages is:

**Algorithm 1: Processing of RREQ and RREP messages**

Begin
a. Initiate route discovery through authentic neighbors (); //RREQ initialization by the source node
b. Processes RREQ (); //RREQ processing at intermediate node
c. Propagates RREQ (); // through its authentic neighbors
d. Generates and unicasts RREP ();
e. Switches to monitoring and identification Routine (); //RREQ processing at target node
f. Modifies and unicasts RREP (); //RREP processing at intermediate node
g. Processes RREP (); //RREP processing at source node
End
4.2 Selfish Node Detection:
The SOMANET is modeled and the nodes in the network are deployed according to the architectural model. Numerous nodes participate in the SOMANET for forwarding and transmitting the data packets between the source and destination. 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. This type of nodes likes to enjoy the profits provided by the resources of other nodes in the network. It does not make its own resource accessible to others. These nodes intend to get the greatest benefits from the network while trying to preserve their own resources. 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.

Existing explorations on selfish behaviors in a SOMANET mainly concentrates on network concerns. The main objective of this analysis is to enhance the performance of SOMANET by detecting these types of selfish nodes using game theory and DTSA technique. In this paper, the problem of selfishness is addressed by trust mechanism using game theory.

5. IMPLEMENTATION:

5.1. Implementation Tool:
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.

5.2. Results and Analysis
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 and false positive rate.

5.2.1. Attack Detection Ratio
Compared to nash method, the proposed strong nash game theory method significantly increases the detection ratio, because it finds the difference between the normal user and the attacker. The comparative analysis between the existing nash and proposed strong nash
method, which is shown in figure 1.0. In this graph, the x-axis represents the number of selfish nodes and the y-axis represents the detection ratio in terms of percentage.

**Figure 1 Detection Ratio**

### 5.2.2. Average Packet Dropping:

The implication of not forwarding the packets or dropping the packets in SOMANET while providing services leads to a serious problem. So, this analysis addresses this event and gives higher priority for packet dropping in SOMANET while providing services. The packet drop rate is observed in the selfish node detection methods; namely, **Trust Based Heuristic Algorithm (THA)** and DTSA. The comparative analysis with respect to the number of nodes is shown in figure 2.0. In this graph, the x-axis represents the number of selfish nodes and the y-axis represents the average for dropping packets.

**Figure 2 Average Packet Dropping**

### 5.2.3 False Positive Rate

The false alarm will be differentiated from the overall selfishness alarm. The detection of this false alarm leads to better performance in the overall network. The probability of parameters such as, energy, memory space and CPU time in packet drop rates are analyzed with respect to the false alarm rate. The comparison between the existing THA and the proposed DTSA technique is shown in figure 3.0. In this graph, the x-axis represents the number of selfish nodes and the y-axis represents the false positive rate in terms of percentage.
In more specific the chapter particularly interested in the total number of data’s and verification delay during a secure data transmission and the average processing time of a verification process since they are the dominant factors affecting service quality experienced by the users.

6. CONCLUSION:
This paper proposed a new attack detection and service allocation scheme for SOMANT, because 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. These misbehaviors of the selfish nodes will have impact on the efficiency, reliability, and fairness. The selfish node utilizes the resources for their own purpose, and it neglects to share the resources to other nodes. So, it is important to detect the selfish nodes in MANET. The paper considered the service oriented attack detection problem on SOMANETs and designing a new game theory driven approach named as DTSA, a honeypot and game theory approaches were deployed for secure service allocation. 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. Additionally the system proposes a new technique, namely, Trust calculation and attack Detection, which helps to detect the selfish nodes in an efficient manner using the honeypot. The suggested method is an effective method, which enhances the performance of MANET. The false positive rate and detection ratio improved significantly and hence reduced the packet dropping. It significantly improves the performance metrics success ratio for query and decreases traffic. The experiments and results show the proposed DTSA mechanism can effectively identify the intruder at the time of data transaction. NS-2 tool has been used for the simulation.

REFERENCES:
Dual Trust Based Service Allocation Protocol for Service Oriented Manet


