ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Heuristic Method against Selfish and Malicious Behavior Attacks in Opportunistic Networks

Santhosh J [1], Malini V K [2]

Assistant Professor, Dept. of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India[1]

M.Phil Scholar, Dept. of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: Wireless networks are infrastructure less, where every node utilizes the opportunistic contact for data communication. Due to the dynamic nature, several security threats arise in such networks. The lack of infrastructure less and dynamic topology makes it impossible to establish a proper connections in ad-hoc networks. In such network store-carry-forward strategy can be employed. But, those routing process depends heavily on the cooperation among other nodes. In the infrastructure free network, the selfish behavior of nodes affects the overall performance of the packet transmission. Selfish or malicious behaviors of nodes impact greatly on the network performance. In this paper, we analyze and design an active trust handling model for secure routing optimization against selfish and energy. In this paper, we focus on both selfish and malicious nodes in opportunistic contact networks. Here the malicious nodes are considered as the energy suckers, where selfish behaviors could be identified easily using existing EBOX. So our proposal improves the reliability among dynamic topological environment against selfish and energy suckers. The above stated problem in opportunistic network is handled by incorporating two mechanism named as evidence collection and acknowledgment verification. This is handled by the heuristic method, where the optimal and prioritized attribute or behavior is considered initially. This reduces the time for the attack detection.

KEYWORDS: Mobile ad-hoc networks, Opportunistic network, Behavior, Trust, Reputation, Selfish attack and energy suckers.

I. INTRODUCTION

In the recent network scenario, opportunistic networks have a unique space and tremendous growth. Here opportunistic network is considered as a challenging environment where the communication and contacts are extremely dynamic and unpredictable nature. The Mobile Opportunistic Networks (MoNet) are an extreme generalization of Mobile Ad-Hoc Networks, which aim at enabling communication between mobile nodes in highly challenged conditions and emergency situations [1]. This opportunistic environment raises many security issues due to several parameters. As in MANET’s nodes are belong to the heterogeneous networks, where the nodes are not relay on the global infrastructures. Due to the heterogeneity nature, nodes don’t have a unique address across the different networks and furthermore raises the requirement for new authentication and trust establishment mechanisms dynamically.

The ad-Hoc networks have high mobility here nodes are affected by certain disruptions. Finding stable and static route is impossible in such networks. As like the routing process, security solutions should adaptable for the dynamic network infrastructure. When considering heterogeneity and mobility, the system should support delay tolerance, this type of attributes are failed to perform secure communication, because these systems adopting a store and forward strategy. In this paper, we propose security architecture to address the selfishness problem in opportunistic networks. In the proposed system, when the source opportunistic network node sends a bundle it doesn’t set a routing path in advance, but only need to attach some inducement on the bundle. Then, the selfish opportunistic network nodes on the network could be stimulated to help with forwarding the bundle to improve the delivery ratio and reduce the average delay of the whole opportunistic networks.

Energy suckers in MONET are referred as the instance of denial of service attack, which drains the nodes energy at the time of transmission [2]. This is performed by the opportunistic forwarder and the attacker may lead the packet on the wrong way or high energy consumed path. In some cases, the attacker will attach bundle of data and re-transmits to the honest node. The honest node transmitted a message to the same destination. This is quite difficult to obtain original packets, because it uses different packet headers. The ratio of network wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant.

II. LITERATURE STUDY

In this section, we discuss security issues of the MONET in various circumstances, i.e., the fairness, the free ride attack, the layer removing attack and the layer adding attack [6]. Note that, since the proposed protocol deals with the selfish opportunistic network nodes in opportunistic networks, and energy suckers in opportunistic network other attacks launched by malicious opportunistic network nodes are out of the scope of this study. Authors in paper [7] have demonstrated that watchdogs are appropriate mechanisms to detect misbehaving and selfish nodes in ad-hoc networks. Broadly, watchdog systems are considered more efficient technique to detect the selfishness. This overhears wireless traffic and analyses it to decide whether neighbor nodes are malicious or not. If the watchdog detects the selfish behavior, then it is highlighted as positive detection else that is marked as non-selfish node. The main drawback of this kind of detection technique is it increases false alarms.

The authors in [8] presented a method using a virtual currency called nuglet. Later author Zhong et al. [9] proposed SPRITE technique which is a credit based system to provide incentive to the participation of selfish nodes in MANET. This type of methods created several issues. The issues are common in the MANET, because storing individual data on the server is very complicated. They can be improved by applying some special tamper proof hardware’s, Later some authors introduce selfish node detection using cooperative concepts. In this approach, every node actively participates in the group activities such as forwarding the data to the receiver. FIP provides incentive to mobile nodes to cooperate in selfish MANETs. It does not require any tamper resistant device and special hardware. This achieves the fairness between the source, destination and intermediate nodes.

The 2ACK technique is based on a simple 2 hop acknowledgment packet that is sent back by the receiver of the next hop link. Compared with other approaches, the 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers. Most of the routing algorithms designed for MANET such as DSR and AODV are based on the assumption that every node forwards every packet. But some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for re-transmitting the data of other nodes and they reserve them only for themselves.

The paper [10] discusses two techniques namely Reputation based technique and Credit based technique used to detect selfish nodes in MANET. In literature, the paper [11] discusses two algorithms that are based on reputation based technique and one algorithm based on credit based technique. Finally all three techniques have been compared. Various algorithms have been designed in recent years to resolve the issue of selfish nodes. Each algorithm takes a different approach to the problem, but the majority of these algorithms can be broken into three general categories. In a reputation based algorithm, each node is responsible for either keeping track of other nodes, or obtaining the reputation from a centralized node on the network. If a node successfully participates in the transmission of data by forwarding data packets, the reputation of the node is increased, or if the node discards the packet by dropping it, the reputation is decreased. After the nodes reputation drops below a threshold set by the developer, the node is either punished or ignored. A credit based algorithm is similar to a reputation based algorithm. The difference is this algorithm is that each node begins with a set of credits. A node sends a packet to its neighbor node for forwarding. After successfully forwarding the packet, the sending node credits the neighbor as a reward. If nodes do not forward the packet, they will run out of credits, resulting in not having the ability to send their own packets.

DOI: 10.15680/IJIRCCE.2016. 0403174

III. PROBLEM DEFINITION

In MoNet, there is no infrastructure and all nodes are expected to take part in the forwarding process in order to increase the communication opportunities. This creates the issue of selfish behavior: nodes are inclined to forward only packets that interest them while ignoring others. This issue is even more critical for small devices as scarcity of resources fosters selfish behavior. Nodes need therefore incentives in order to cooperate with each other for fine communications. This issue has already been studied for MANETs but the solutions proposed cannot apply to MONET. Our proposal fully concentrated on the two main security issues in MONET, such as selfish attack and energy suck problem.

Really, currency based cooperation enforcement schemes rely either on costly tamper-proof hardware [3] or on an online trusted third party [4] which is not compatible with the delay tolerance characteristic, while reputation mechanisms like [5] require stable network configuration and a large amount of time to establish trust.

IV. PROPOSED SYSTEM

There is several studies implemented solution against selfish attacks; however the detection of selfishness is easier than protecting that. We therefore proposed a new approach to enforce cooperation that fits MONET requirements. This solution is based on the previous EBOX approach where nodes have to take a decision of accepting to receive a packet and paying for it or not blindly. If the node then discovers that the packet is not interesting for him, it is incited to forward the packet to other nodes in order to get its payment back, hence cooperation is enforced. This protocol achieves optimistic fair exchange: if a conflict occurs an authority guarantees fairness by giving each party its rightful part, but the authority is not required in case of correct execution of the protocol. This protocol sketch shows that this approach is suitable for MONET because it does neither require prior trust establishment nor online authority and it is flexible: nodes can decide not to receive packets , it considered as its resources are low, but in this case they might miss packets destined to them, or they can decide to collaborate with others to receive packets destined to them and forward other packets and thus aim to drop energy of other nodes.

At the same time, the proposal also deals with the energy suckers, where the energy is drained by some malicious intermediates.

Opportunistic networks are typically characterized by the unguaranteed connectivity and the low frequency of encounters between a given pair of nodes within the network. In our proposed system, we consider an opportunistic network as a directed graph G = (V, E), where V and E represent the set of opportunistic network nodes and opportunistic contact edges, respectively. In the opportunistic network, a source S can deliver packets to a destination D via the movement of opportunistic network nodes with proper data forwarding algorithm. Currently, contingent upon whether they allow multiple copies of a message relaying within the network, the existing data forwarding algorithms may be categorized into single-copy and multi-copy algorithms. In the single-copy algorithm, only one copy is relayed in the network until it arrives at the destination. While in the multi-copy algorithms, such as flooding or spray routing, more than one copy are relayed in the networks. Due to large number of message copies in the networks, this kind of approach consumes a high amount of resources which are scarce in opportunistic networks. In this work, in order to clearly illustrate the practical enticement, we just consider a single-copy data forwarding algorithm, i.e., for each bundle B, only one copy is initially spread by the source S, and then the only copy is opportunistically relayed from one forwarding node to another until it's reaching the destination D.

```
Heuristic based approach:
(1) Compute an initial permutation O = O1,O2,...,On
(2) For j = 1,2,...,n:
        Evaluate all possible insertions move(Oj,i).
        Let move(Ok,i ∗) be the best of these moves.
        If move(Ok,i ∗) is improving then perform it and update O.
(3) If some improving move was found, then goto (2).
```

Algorithm 1.0 Heuristic approach

In MONET, the selfish behaviors of opportunistic network nodes are naturally caused by human entities that control them. In our proposed system, in order to study the selfish and energy sucker opportunistic network nodes, we take Mobile opportunistic network (MONET), where each opportunistic network node is instantiated by mobile node driven by users using their devices. Therefore, there may arise many selfish opportunistic network nodes in the networks, if not there may be energy sucker. In order to conserve buffer space, these selfish opportunistic network nodes may be very hesitant in the cooperation that is not directly beneficial to them. As a result, the selfishness would be against the goal of the mobile opportunistic network to cooperatively deliver a bundle from its source S to the destination D. Therefore, the cooperation probability of a selfish opportunistic network node should be identified.

The main design goal of out proposed system is to develop a new technique to stimulate the selfish opportunistic network nodes to improve the cooperation probability Pc in the networks along with the detection of energy suckers. Specifically, the following two desirable objectives will be achieved. · Improving opportunistic network's performance with stimulation: In order to prevent the overall performance degradation, i.e., low delivery ratio and high average delay, due to the selfish opportunistic network nodes in MONET, the credit-based enticement strategy is adopted. The detection of selfish and energy suckers are incorporated with several behaviors. Verifying every behavior to find the selfish node is a complicated on in MONET. So we proposed a Heuristic method, which helps to select an optimal attribute among the total list.

Enticement Strategy: To achieve the above objectives, the following Heuristic strategy is adopted. · There exists a trusted authority (TA) in the system similar to EBOX. Although it does not participate in bundle forwarding in opportunistic networks, TA performs trusted fair credit and reputation clearance for opportunistic network nodes. Therefore, before joining the opportunistic networks, each opportunistic network node should register itself to the TA and obtain its personal credit point and personal reputation point in the initial stage.

In mobile networks, selfish behavior identification is a challenging part, where every node behaves differently and the detection from those behaviors is complicated. The proposed work performs the following steps to detect the selfish and energy drainers in the network. Due to different functionalities in every network, Local Search Methods (LSM) heuristic approach is used. The local search starts with some feasible solution of the selfish node detection problem. At every iteration, the system finds optimal solution. Our main aim is to reduce the effort to detect the selfish node. The method terminates when, for a solution, there is no other accessible solution that improves it.

V. IMPLEMENTATION AND RESULTS

The proposed system is simulated on Network Simulator (NS2) Platform. Network simulation is one of the most widely used ways to evaluate the network routing protocols. The working of Secure Routing Protocol in MONET against selfish and energy sucker attackers is explained is that messages in ad hoc network must be authenticated to guarantee the integrity and non-repudiation so that the protocol and nodes can be prevented against several kinds of attacks

We used the software of NS-2 to evaluate the malicious behavior of the attacks and performance of proposed work. The parameters of our simulation are given in the Table 1.0.

Parameter	Value
Simulator	NS 2.35
Simulation duration	300 sec
Number of nodes	50
Routing Protocol	AODV
Topography	1000 m and 1000m
Packet size	512
Initial Energy	2 J

Table 1.0 simulation parameters

We focus on parameters quoted below to study the attacks .In Selfish as well as in energy sucker the number of sent packets is lower than the number of received packets so these parameters are chosen and the energy suckers are the intermediate node drains the node energy abnormally. The energy consumption differs for Overflow because each received packet corresponds to a loss of energy. The parameters are:

a) The number of packets sent

b) The number of packets received

c) The number of packets lost

d) The consumption of energy.

e) The attack detection rate

The rate of lost packets is equal to the number of lost packets divided by the number of sent packets. The output is the number of received packets divided by the number of sent packets in the application layer.

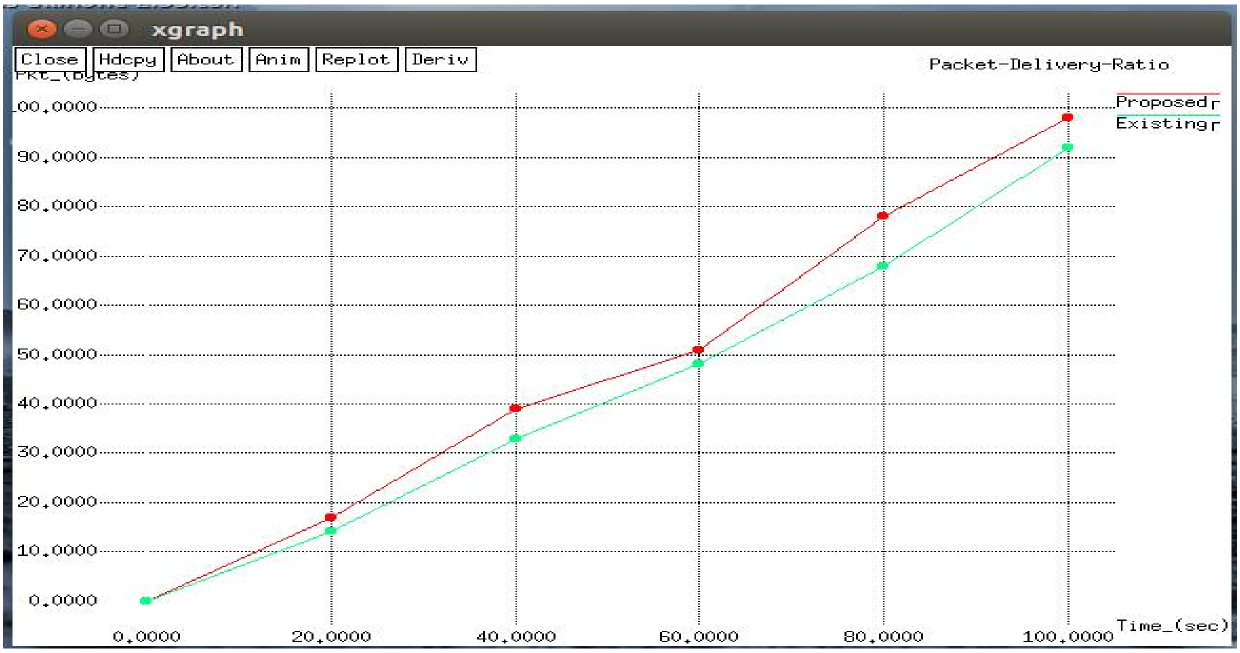
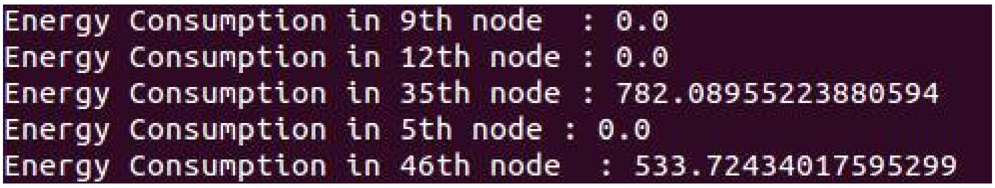


Fig 1.0 Packet delivery ratio comparison graph

From the above simulation parameters, the 50 nodes are initiated and performed the simulation. Where the simulation taken with two type of attackers such as energy suckers and selfish behavior. The proactive nature of our approach detects the attacker node at earlier stage using heuristic approach. So the packet delivery ratio is increased in our proposed scheme.



```
Energy Consumption in 9th node  : 0.0
Energy Consumption in 12th node : 0.0
Energy Consumption in 35th node : 782.08955223880594
Energy Consumption in 5th node : 0.0
Energy Consumption in 46th node  : 533.72434017595299
```

Fig 2.0 Energy analysis at every node (energy specified in MJ)

In order to find the malicious behavior of intermediate node, the system calculates the average energy taken at every node. If the behavior related to the energy is deviated, then the node's credit points will be minimized.

VI. CONCLUSION

The state-of-the-art wireless networks such as Mobile Ad hoc Networks (MANET) and Mobile Opportunistic Networks (MONET) are highly dynamic and depend greatly on routing and network layers. Due to this dynamic nature, Mobile networks are extremely vulnerable for several attacks. There are several works in the literature proposed reputation and behavior based selfish attack detection in MANET. We proposed a new heuristic based approach to detect selfishness and energy suck attacks in MONET. In this type of networks, the nodes are too dynamic, so calculating and maintaingng reputation score and finding attacks consumed much time and cost. Our aim is to create a simple and cost effective technique to relay in selection of methods which is appropriate to the current scenario. The basic analysis and implementation is performed in NS2 simulator tool. And the basic results are obtained with various test considerations. Finally the system provides an optimal solution against the two types of attacks from the list of solutions.

REFERENCES

1. Pelusi, Luciana, Andrea Passarella, and Marco Conti. "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks."*Communications Magazine, IEEE* 44.11 (2006): 134-141.
2. Kumar, D. Naveen, and B. Purushotham. "Methods to Mitigate Vampire Attacks from Wireless Ad-hoc Sensor Networks." (2014).
3. Marias, Giannis F., et al. "Cooperation enforcement schemes for MANETs: A survey." *Wireless Communications and Mobile Computing* 6.3 (2006): 319-332.
4. Irshad, Azeem, et al. "Security Enhancement in MANET Authentication by checking the CRL Status of Servers." *Int J Adv Sci Technol* 1 (2008): 91-98.
5. S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.
6. Shikfa, Abdullatif. "Security issues in opportunistic networks." *Proceedings of the Second International Workshop on Mobile Opportunistic Networking*. ACM, 2010.
7. Spyropoulos, Thrasyvoulos, Konstantinos Psounis, and Cauligi S. Raghavendra. "Efficient routing in intermittently connected mobile networks: the multiple-copy case." *Networking, IEEE/ACM Transactions on* 16.1 (2008): 77-90.
8. Zhang, Yanchao, et al. "A secure incentive protocol for mobile ad hoc networks." *Wireless Networks* 13.5 (2007): 569-582.
9. 8. Anderegg, Luzi, and Stephan Eidenbenz. "Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents."*Proceedings of the 9th annual international conference on Mobile computing and networking*. ACM, 2003.
10. 9. S. Zhong, J. Chen, and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE Conf. Comput. Commun., Mar. 2003, vol. 3, pp. 1987–1997.
11. Y. Yoo, S. Ahn, and D. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks," in Proc. IEEE Int. Conf. Commun., May 2005, vol. 5, pp. 3005–3009.