Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 121-126, 2016
ISSN 1990-9233;
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.TAET23333

# Token Ring Based Co-Operative Bait Detection for Both Selfish and Malicious Node Attacks In Ad Hoc Network Communication

*[1]A. Syed Musthafa, [2]Dr. C. Nelson Kennedy Babu and [3]R. Kasthuri*

[1]Assistant Professor Department of IT, K.S.Rangasamy College of Technology, Tamilnadu, India
[2]Professor, Department of CSE, DhanalakshmiSrinivasan College of Engineering, Tamilnadu, India
[3]PG Scholar, Department of IT, K.S.Rangasamy College of Technology, Tamilnadu, India

**Abstract:** Mobile ad hoc networks (MANETs) nodes assist with each other for efficient communication between them. The presence of malevolent nodes, node cooperation direct to severe security problems and the malicious nodes disturb routing process. Preventing or detecting malicious nodes show the way to gray whole or collaborative black hole attacks.Dynamic source routing method handles security problems on cooperative node communication in MANET. The existing work presented Cooperative bait detection scheme (CBDS) which integrates both proactive and reactive defense architectures and it develops a reverse tracing method. CBDS overcomes state of art of existing routing protocols DSR and 2ACK best-effort fault-tolerant routing (BFTR) protocols.Destination address is used by the adjacent node to attract malicious nodes and also to send a reply RREP message. The malicious nodes are found by reverse tracing method. However the method is incapable to detect selfish node attacks. It provides only average throughput on data delivery and increased routing delay on internal attacks. Also it consumes more attack detection time for multiple attacks. To overcome these drawbacks, the proposed method presents Token Ring based Co-operative Bait Detection for both Selfish and Malicious Node Attacks in Ad Hoc Network Communication to find selfish node attack in MANET. Ring of tokens are developed to attract the selfish nodes and malicious nodes. Source node provides ring of tokens using pseudo random function and issued to the reputed neighbor node.Tokens developed in two rings of various sequential orders selfish nodes are in one sequential order (in one ring) and the malicious node are in another sequential order (in another ring). Neighbor nodes arrived tokens induce bait route demand to all other nodes with bait tokens.

**Key words:** MANET · Ad Hoc Network · Cooperative bait detection scheme

## INTRODUCTION

A Mobile Ad hoc Network (MANET) consists of a number of mobile hosts that connect each other through wireless communication. A packet typically has to go many hops before reaching its destination. Therefore, every mobile host in such a network has the obligation to behave on demand as a router to ensure the packet delivery. Mobile ad hoc networks (MANETs) consist of a collection of mobile nodes which can move freely. Many routing protocols, such as Ad hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR), have been used for MANETs. The CBDS technique provides a reverse tracing technique to aid in obtaining the stated goal. This method aids in defending in opposition to the blackhole attack with no condition of hardware and special detection node. Here, a method called cooperative bait detection scheme (CBDS) is developed to effectively find the malicious nodes that tries to begin grayhole or collaborative blackhole attacks. In this technique, the address of a nearby node is used as bait destination address to bait malevolent nodes and to send a respond RREP message. The malicious nodes are found by reverse tracing method. The malicious nodes are set aside in a blackhole register to alert the participant of the routing message to stop linking with the nodes in that record. The advantage of CBDS relies to combines the proactive and reactive defence architectures to attain the aforementioned goal.

**Corresponding Author:** A. Syed Musthafa, Assistant Professor Department of IT,
K.S. Rangasamy College of Technology, Tamilnadu, India.

**Literature Review:** In this paper [1], the author described about Cooperative bait detection scheme that matches proactive and receptive protection architectures and randomly collaborates with stochastic nearby node. The address of an adjacent node is employed as bait destination address to the malicious nodes to transmit a reply message (RREP). Strange nodes are identified using reverse tracing technique thus prevents and ensures security.

In this paper [2], the author propose a Cooperative Bait Detection Scheme (CBDS) using DSR protocol to detect malicious nodes to initiate gray /collaborative black hole attacks in MANETs. The CBDS scheme incorporates the proactive and reactive defense architecture and randomly collaborates with a stochastic adjacent node. The address of an adjacent node as bait target address to attract malicious nodes to transmit a reply message (RREP) and detected strange nodes with reverse tracing technique to prevent and ensures security.

In this paper [3], author described aboutA Survey on Secure Cooperative Bait Detection Approach for Detecting Malicious Nodes in MANETs. The problem of security with formation of communication nodes is executed together with each other. Preventing or sensing malicious nodes launching gray whole or collaborative black hole attacks is the main challenge. Cooperative bait detection approach combines both proactive and reactive defense architectures.

In this paper [4] the author studies mobile ad-hoc network and its characteristics, challenges, application, security goals and different type's security attacks at different layers. Security attack can organized into two types of attacks such as active or passive attacks. Different security mechanisms are introduced to prevent such network.

In this paper [5], the authorintroducesMobile Ad Hoc Networking to provide complete dynamic field. Initially, the mobile ad hoc networks are executed in evolution of future wireless technologies. Afterward, the most research activities in these areas of Manet's characteristics, capabilities and applications are analyzed.

In this course [6], the author initially considering current protocols which give connectivity in mobile ad hoc networks, such as routing and MAC protocols. Then, the author will also cover an emerging area within Sensor Networks and explained broad significance. Finally, the current challenges are discussed to mobile networking and highlighting some current wireless protocol standardization efforts in IETF and the Bluetooth SIG (Special Interest Group).

The essential idea of this paper [7] is to illustrate information theoretic models for cooperation, possible rate regions and outage probabilities. Subsequently, the channel coding techniques are applied to exploit the diversity advantages of cooperation. Cooperative communication provides processing of overheard information at the neighboring nodes and retransmission nears the destination to generate spatial diversity, therefore achieve throughput rate and reliability.

This work [8] presents a solution to classify malicious nodes in WSN via detection of malicious message transmissions in a network. A message transmission is considered distrustful if its signal strength is mismatched by originator's geographical position.

This paper [9] provides a protocol for routing in ad hoc networks to utilize DSR. This protocol rapidly alters the routing protocol when host movement is repeated. However, a host travel less frequently and does not overhead during periods. The packet-level simulation of mobile hosts in ad hoc network, the protocol achieves different environmental conditions are host density and movement rates.

This paper [10] studies the measures of selfish nodes concentration on the quality of service in MANETs. The authors specify in detail how the different nodes are cooperate with the local reputation values to a global reputation and how response to negative reputations of nodes.

This paper [11] outlines main attacks and reviews popular approaches to plan secure MANET protocols that detect selfish and malicious nodes to implement cooperation. The base stations and central services are one of the main issues during implement a MANET since it is determines the choice of protocols. The base stations are attached to access other nets and many services implemented by distributed algorithms. Therefore, it reduces redundancy cost and better accessibility of single access points.

In this paper [12], the classification of cryptographic random number generators (RNGs) is presented. With five different examples of practical generators such as /dev/random, Yarrow, BBS, AES and HAVEGE is provided. Then, the three mathematical theories are designed used in connection with random number generators. The mathematical theories are randomness and address Shannon's entropy, Kolmogorov complexity and polynomial-time indistinguish ability.

The essential idea of this paper [13] is developed to efficient security decision on data protection, secure routing and other network activities by using trust evaluation based security solution. Logical and computational trust analysis and evaluation are organized with network nodes.

In this paper [14], the effect of selfish node attack on AODV is analyzed. For this analysis, there are 50 nodes are chosen and among these, there are 5 nodes are chosen as selfish nodes. The simulation is carried out in Riverbed Modeler and various performance parameters are studied. It is observed that, initially there is very less data loss in the AODV network.

In this paper [15], the author studies certain collaborative attacks in MANET. Finally, the collaborative attacks compared to some other attacks using some important parameters and then addressed major issues related to this. The block whole attack affects the performances of several MANET applications. These attacks mainly target on the way of the data packets and hack it.

Therefore, this accurate information cannot be delivered to the desired destinations and significantly reduced performance of network. As a result, in future different routing protocols for MANET is considered to perform comparative study and improve the performance of routing protocols for MANET to prevent Black hole attacks.

**Token Ring Based Co-Operative Bait Detection for Both Selfish and Malicious Node Attacks in Ad Hoc Network Communication:** This work designs a Token Ring based Co-operative Bait Detection scheme for identifying selfish node attack in MANET. The token rings are developed to both bait the selfish nodes and malicious nodes. By using pseudo random function, the source node generates ring of tokens and distributed to the reputed neighbor node. The Node's with trusted communication history are planed as reputed nodes and check the reputation count of the nearest neighbor node to distribute the ring of tokens. The Tokens rings are classified into two different sequential orders such as selfish node is one sequential order and malicious node is another sequential order. Once the neighbor nodes are received, the tokens are simulated route request to all other nodes with bait tokens.

All other nodes are including selfish and malicious node to send the reply to corresponding source node. By introducing Back tracking algorithm is used to discover the reputation node from selfish node and malicious node. With arrived reply along its tokens issued from source node request, ring of selfish nodes and malicious node are identified using external adversaries.

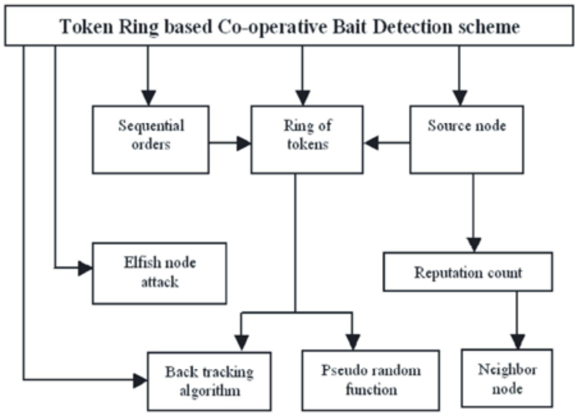

Fig. 3.1: Architecture Diagram for Token Ring based Co-operative Bait Detection scheme

With objective of improving throughput on data delivery and reduce overhead thereby minimized attack detection time for different type of attack such as selfish node, black hole and grey hole attacks.

The proposed scheme is divided into three phases namely:

- Ad Hoc Network Communication
- Selfish Nodes and Malicious Node Attacks
- Token Ring Co-operative Bait Detection

**Ad Hoc Network Communication:** A mobile ad hoc network (MANETs) is generally used for several applications such as military crisis operations, emergency preparedness and response operations. In Ad hoc network communication, each node not only generates as a host also act as a router along with nodes needs cooperation with each other to forward data packets. Cooperative communication features provide issues on security aspect. Ad hoc network communication requires stringent constraints on security features. The security features such are:

- Network topology
- Routing
- data traffic

**Selfish Nodes and Malicious Node Attacks:** The malicious nodes attacks attract all packets by using Route Reply (RREP) packet that fake shortest route to the destination and avoid these packets without forwarding them to destination. Certain malicious node turns malicious only at a specific time for preventing trust-based security solution in the network. But selectively rejects/forwards the data packets once packets go through it.

Selfish Nodes are generated and does not participating in routing process in order to drop routing messages and modify the Route Request. In addition to Reply packets are changed by TTL value to smallest possible value. Moreover, the Selfish Nodes cannot answer the send messages significantly detected other unable nodes. With objective of delay RREQ packet helps to maximum upper limit time and avoid falls data packet from routing paths.

**Token Ring Co-operative Bait Detection:** The selfish node and collaborative attacks are detected using dynamic source routing (DSR) routing. Circular ring of tokens are generated to bait selfish nodes and malicious nodes. The mobile nodes provides ring of tokens using Pseudo random generationand issued to the neighbor node.Each node with trusted communication history is listed. Nodes with trusted rating high are termed as reputed nodes and ring tokens issued to nodes with higher reputation count. The tokens generated into two different sequential orders such as selfish nodes in one sequential order and malicious node in another sequential order.

Once token neighboring nodes are received to simulate bait route request to all other nodes with bait tokens and all other nodes including selfish and malicious node send to reply corresponding source node. Then, back tracking algorithm is applied to identify the route path from different type of nodes such as,

- Reputation Node
- Selfish Node
- Malicious Node

**Performance Metrics:** In this section evaluate the performance of Token Ring based Co-operative Bait Detection for both Selfish and Malicious Node Attacks in Ad Hoc Network Communication. One of the major contributions of this work is to prevent selfish node attacks and malicious nodes attack in MANET for routing overhead. The performance metrics of the parameters is number of selfish nodes detected, malicious node density, Throughput on Data Forwarding, Routing Overhead and Average Delay Time.

The performance metrics are:

- Throughput rate
- Routing Overhead
- Average Delay time

**Throughput Rate:** Ad hoc networks comprise of group of nodes to communicate with each other over wireless channel. The nodes collaborate in routing the data packets from the transmitting node to the intended destination node. The network self-interference model is used to identify the network throughput. The throughput rate in ad hoc networks extensively used in many different mobility models. Moreover the global mobility, the each node travels around in the entire network and results in constant per-node throughput.

Table 1: Malicious Node DensitiesVs Throughput On Data Forwarding

| Malicious node densities | Throughput rate on data forwarding | |
|---|---|---|
| | CBDS (Existing) | TR-CBDS (proposed) |
| 10 | 21 | 22 |
| 20 | 25 | 27 |
| 30 | 29 | 33 |
| 40 | 31 | 37 |
| 50 | 34 | 39 |

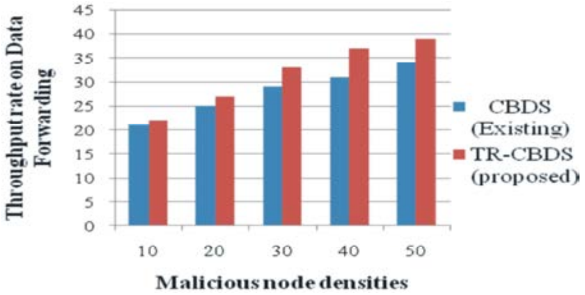

Fig. 4.1: Malicious node densitiesVs Throughput rate

Figure: 4.1. Demonstrate the rate of Throughput. X axis represents malicious node densities whereas Y axis denotes the Throughput rate using Cooperative Bait Detection scheme (CBDS) and our proposed Token Ring based Co-operative Bait Detection (TR-CBDS). When the Malicious node density increased, the Throughput rate is also increased accordingly. The rate of the throughput is demonstrated using the existing CBDS and proposed TR-CBDS method. Figure 4.1. shows better performance of Proposed TR-CBDS provides Throughput rate compared to existing CBDS method. The Token Ring based Co-operative Bait Detection method achieves 10 %high performance of throughput rate when compared with existing system.

**Routing Overhead:** Routing overhead is the number of routing packets required for network communication. Routing overhead is analyzed for determining reactive routing protocols in wireless ad hoc networks. Routed protocol is used to send application traffic. It gives appropriate addressing information in its Network Layer addressing to allow a packet to be forwarded from one network to another.

Table 4.2: Malicious Node DensitiesVs Routing Overhead

| Malicious node densities | Routing overhead | |
|---|---|---|
| | CBDS (Existing) | TR-CBDS (proposed) |
| 10 | 56 | 45 |
| 20 | 58 | 48 |
| 30 | 62 | 51 |
| 40 | 64 | 53 |
| 50 | 65 | 67 |

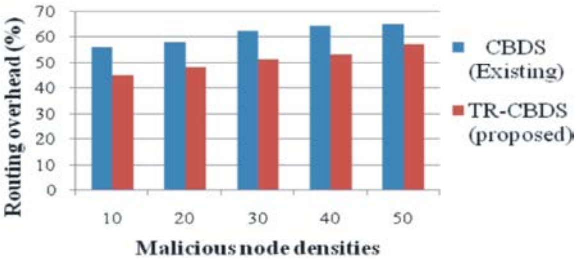

Fig. 4.2: Malicious node densitiesVs routing overhead (%)

Figure: 4.2 Show the routing overhead. X axis represents the malicious node densities whereas Y axis denotes the routing overhead using both Cooperative Bait Detection scheme (CBDS) and our proposed Token Ring based Co-operative Bait Detection (TR-CBDS). When the Malicious node densitiesincreased, the routing overheadgets decreases consequently. The routing overheadis illustrated using the existing CBDS and proposed TR-DBDS Technique. Figure 4.2. illustrates better performance of Proposed TR-CBDS method in terms of node densitiesthan existing CBDS and proposed TR-CBDS. The Token Ring based Co-operative Bait Detection scheme achieves 20 % of routing overhead when compared with existing system.

**Average Delay Time:** The average delay time in identifying the attacks is measured using the routing nodes and time for identifying the attack. The average delay time in identifying the attacks is measured in terms of milliseconds (ms) and analyzed delay time during packet transmission. The average delay time also includes the delay caused for route discovery and queue observed during the transmission of data packet

Table 3: Malicious Node DensitiesVsAverage Delay Time

| Malicious node densities | Average delay time | |
|---|---|---|
| | CBDS(Existing) | TR-CBDS (proposed) |
| 10 | 12 | 10 |
| 20 | 15 | 13 |
| 30 | 19 | 15 |
| 40 | 21 | 17 |
| 50 | 25 | 19 |

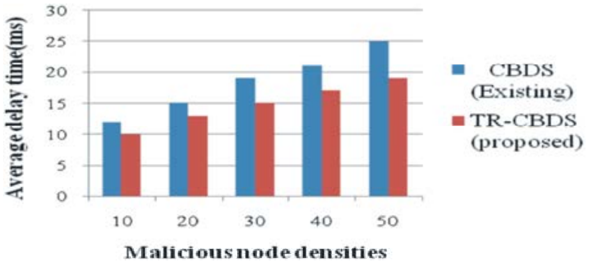

Fig. 4.3: Malicious Node DensitiesVs Average Delay Time (Ms)

Figure 4.3 Illustrate the average delay time. X axis represents the malicious node densities whereas Y axis denotes the Average delay time using both the Cooperative Bait Detection scheme (CBDS) and our proposed Token Ring based Co-operative Bait Detection scheme (TR-CBDS). When theMalicious node densities increased, average delay time gets decreases accordingly. The time of the average delay is illustrated using the existing CBDS and proposed TR-CBDS method. Figure 4.3. shows better performance of Proposed TR-CBDS method in terms of node densitiesthan existing CBDC and proposed TR-DBDC. The Token Ring based Co-operative Bait Detection (TN-CBDC) method achieves 23 % high performance of average delay time when compared with existing system.

## CONCLUSION

This paper proposes a Bait Detection scheme for both Selfish and Malicious Node Attacks in Ad Hoc Network Communication. It is discovering the selfish node attack in MANET. Initially Ad hoc network communication provides security elements such as network topology, routing and data traffic to deliver the packets. The Ring of tokens is introduced to detect selfish node attacks along with malicious node to improve throughput rate and reduced routing overhead with delay. The performance of proposed Token Ring based Co-operative Bait Detection schemes are done with following metrics through the NS2 simulator.

## REFERENCES

1. Prachi Arya and Gagan Prakash Negi, 2015. Pushpender Kumar Dhiman and Kapil Kapoor, “CBDS (Cooperative bait detection scheme) ATTACK-A Review”, International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 4(8), August 2015, pp: 3428-3434.
2. Akinlemi Olushola, O. and K. Suresh Babu, 2015. “Cooperative Bait Detection Scheme (CBDS) To Avoid the Collaborative Attacks of Nodes in MANET”, International Journal of Scientific Engineering and Research (IJSER), 3(4), April 2015, pp: 66-69.
3. Mohan, M. and M. Ramakrishna, 2015. “A Survey on Secure Cooperative Bait Detection Approach for Detecting Malicious Nodes in MANETs”, International Journal on Recent and Innovation Trends in Computing and Communication, 3(3), March 2015, pp: 1066-1069.
4. Aarti and Dr. S.S. Tyagi, 2013. “Study of MANET: Characteristics, Challenges, Application and Security Attacks”, International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), May 2013, pp: 252-257.
5. Pravin Ghosekar, Girish Katkar and Dr. Pradip Ghorpade, 2003. “Mobile Ad Hoc Networking: Imperatives and Challenges”, Elsevier, Ad Hoc Networks, 1(1), July 2003, pp: 13-64.
6. Carlos de Morias Cordeiro and Dharma P. Agrawal, 0000. “Mobile Ad hoc Networking”, pp: 1-63.
7. Elza Erkip, Andrew Sendonaris, Andrej Stefanov and Behnaam Aazhang, 0000. “Cooperative Communication in Wireless Systems”, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, pp: 1-18.
8. Waldir Ribeiro Pires Junior, Thiago H. de Paula Figueiredo, Hao Chi Wong and Antonio A.F. Loureiro, 2004. “Malicious Node Detection in Wireless Sensor Networks”, Proceedings of 18th International Parallel and Distributed Processing Symposium, pp: 7.
9. David, B. Johnson and David A. Maltz, 0000. “Dynamic Source Routing in Ad Hoc Wireless Networks”, Springer, Mobile Computing, 353: 18.
10. Shailender Gupta, C.K. Nagpal and Charu Singla, 2011. “Impact of Selfish Node Concentration in MANETs”, International Journal of Wireless and Mobile Networks (IJWMN), 3(2), April 2011, pp: 29-37.
11. Martin Schütte, 0000. “Detecting Selfish and Malicious Nodes in MANETs”, pp: 1-7.
12. Andrea Rock, 2005. “Pseudorandom Number Generators for Cryptographic Applications”, March 2005, pp: 123.
13. Zheng Yan, Peng Zhang and Teemupekka Virtanen, 0000. “Trust Evaluation Based Security Solution in Ad Hoc Networks”, Proceedings of the Seventh Nordic Workshop on Secure IT Systems, pp: 1-14.
14. Mani Bharathi, Ranjith Sairam, S. Sundar and C.M. Vidhyapathy, 2015. “Securing AODV Protocol from Selfish Node Attack”, ARPN Journal of Engineering and Applied Sciences, 10(12), July 2015.
15. Umesh Kumar Singh, Kailash Phuleria, Shailja Sharma and D.N. Goswami, 2014. “A Comparative study of Collaborative Attacks on Mobile Ad-Hoc Networks”, International Journal of Emerging Technology and Advanced Engineering, 4(8), August 2014, pp: 183-187.