Indian Journal of Science and Technology, *Vol 9(41), DOI: 10.17485/ijst/2016/v9i41/94793, November 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Improved Cooperative Bait Detection Method using Multiple Disjoint Path Technique

Chetan S. Arage*, K. V. V. Satyanarayana and J. Amudhavel

Department of CSE, Koneru Lakshmaiah Education Foundation (KLU), Vaddeswaram, Guntur – 522502, Andhra Pradesh, India; chetan.arage@gmail.com, kopparti@kluniversity.in, info.amudhavel@gmail.com

Abstract

The important aim of this research is to present the bait detection method for Mobile Ad Hoc Networks (MANETs) with goal of security and routing performance improvement. **Methods/Statistical analysis:** The proposed method is based on recently presented technique known as CBDS (Cooperative Bait Detection Scheme) which have been introduced for defending against different types of attacks in MANET. The practical analysis of CBDS method is conferred that performance of end to end delay and packet delivery ratio is poor in presence of attacks in network. Therefore, in this paper, improved CBDS (ICBDS) method is proposed with goal improving end to end delay and PDR performances. **Findings:** The simulation and practical analysis of the proposed ICBDS method is done using NS2 tool by considering the different network scenarios and attacks. The results of proposed work against existing CBDS methods claim that the performance of end to end delay and PDR is improved for any numbers of attackers in network. ICBDS technique overcomes the limitations of existing CBDS technique while preserving the MANET security as it is using disjoint path method. The performance of end to end delay is minimized by approximately 22 % whereas PDR performance is increased by 17 % approximately. **Application/ Improvements:** The application area for this proposed method is local banking operations, military application etc. The possible improvement to ICBDS technique will be the consideration of all types of MANET attacks.

Keywords: Attacks, Bait Detection, CBDS, Disjoint Path, MANET Security

1. Introduction

Now days recent several solutions have been introduced for addressing the wireless networks attacks, performance degradations and lower output for those networks. that each one in such kind of conditions we want to possess smart IDS (intrusion detection system) mechanism in area to secure the wireless networks. In[1], projected a unique IDS named EAACK protocol specially planned for the MANETs and differentiated it against existing solutions. In[2], proposed TWOACK security technique for MANET. The TWOACK theme with success solves the receiver collision and restricted transmission power problems which is exposed by the Watchdog. However, the acknowledgment system needed in each packet transmission method additional a major quantity of unwanted network overhead. because of the restricted battery power nature of MANETs, this type of redundant transmission system will normally degrade the lifetime of the whole network. However, several analysis studies have been operating in energy harvest to affect this drawback. In[3] proposed a theme named Watchdog that aims to enhance the output of network with the current of the malicious nodes. As into the fact, the Watchdog theme is consisted of two various elements, namely, Watchdog and Pathrater. Watchdog is an ID for MANETs. several following analysis studies and implementations have established that the scheme of the Watchdog is the economical. moreover, compared to another schemes, Watchdog is capable of detective work malicious nodes is instead of the link. Watchdog theme fails to discover malicious misconducts with the presence of the following: 1) receiver collisions 2) ambiguous

**Author for correspondence*

collisions 3) false misbehaviour report 4) restricted transmission power 5) collusion; and 6) partial dropping. In[4], proposed the recent theme known as AACK supported TWOACK. the same as TWOACK, AACK is a based on the acknowledgment network layer scheme which have been thought of as a mixture of a theme known as TACK (identical to TWOACK) and an end-to-end acknowledgment theme known as acknowledge (ACK). Compared to TWOACK, AACK considerably reduced network overhead whereas still capable of maintaining or maybe surpassing an equivalent network output. The conception of adopting the hybrid scheme into the AACK ultimately decreasing the network overhead, however each TWOACK and AACK still suffer from the matter that they fail to discover malicious nodes with the presence of false misconduct report and cast acknowledgment packets.

In[5], proposed a 2ACK theme for the detection of routing misconduct in MANETs. during this theme, two-hop acknowledgement packets has been sent within the other way of the routing path to point that the data packets are with success received. A parameter acknowledgment ratio, i.e., Rack, is additionally utilized to management the ratio of the received data packets that the acknowledgment is needed. This theme belongs to the category of proactive schemes and, hence, produces further routing overhead consist of the existence of malicious nodes. In [6], projected an interference mechanism known as Best-effort Fault-Tolerant Routing (BFTR). Their BFTR theme uses end-to-end acknowledgements to observe the standard of the routing path (calculated into the conditions of the packet delivery ratio and delay) to be chosen by the destination node. If the behaviour of the trail deviates from a predefined behaviour set for crucial "good" routes, the supply node uses a recent route. one amongst the drawbacks of BFTR is that malicious nodes should still exist within the new chosen route, and this theme is susceptible to recurrent route discovery processes, which can result in vital routing overhead. In [7–9] conferred proactive detection schemes, that are schemes that require to perpetually discover or monitor closed nodes. In these schemes, consist of the existence of malicious nodes, the overhead of detection is consistently created, and therefore the resource used for detection is consistently wasted. However, one amongst the benefits of those kinds of schemes is that it will assist in preventing or avoiding the attack in its initial stage. In [10,11] conferred the reactive detection strategies, those who trigger only the destination node detects a major come by the packet delivery ratio. In[12], projected the recent technique for defensive against cooperative malicious attacks by with the use of CBDS approach on DSR protocol. Author proposed new mechanism (called the CBDS) for detection malicious nodes in MANETs underneath Gray/collaborative black hole attacks. the sensible simulation results discovered that the CBDS outperforms the DSR, 2ACK, and BFTR schemes, given the benchmark schemes, into the terms of routing overhead and the packet delivery ratio. This method is outperforming all existing techniques. The limitation of this method is that poor delay performance; also end to end data security is not considered which may be addressed using efficient cryptography technique only. There are some other methods in [13–18] did work over MANET security.

However, each method is suffered from limitations like when group mobile attackers performing the collaborative attack on MANET, existing methods performing worst to detect and prevent such attacks. To overcome these issues, in [3] novel Cooperative Bait Detection Method to defend against such attacks efficiently. From practical results of this method, it is showing that delay is still more in different network scenarios, also this method does not use any cryptography technique to secure transmission of data. These become new research problem under this domain. In this paper we proposed the improved CBDS method which is based on existing CBDS method by using multiple disjoint paths from source to destination while providing security against different network attacks with goal of reducing the traffic load and hence end to end delay. This proposed protocol we named as ICBDS technique which is compared in this paper against existing schemes such as CBDS and DSR. In rest of paper, section 2 of this paper presenting and discussing methods and materials proposed. In section 3, results and discussion is carried out during this section of paper. Finally, conclusion is presented in section 4.

2. Materials and Methods

2.1 Problem Definition

For real time wireless communications many routing protocols are presented with various goals and the objectives. The operation of this type of routing protocols is majorly depending on mobile devices for routing opera-

tions as well as hosting data. Each routing protocol is by default trusting on mobile nodes for efficient network communication. In real time environment, such mobile networks are open nature which is resulted into the possibility of different types of network attacks purposefully to get important information leakage or misuse. The well-known attacks those are frequently performing on mobile ad hoc network are malicious node attacks like selfish node, black hole node etc. Denial of Service (DoS) attacks etc.

The main reasons behind such attacks are that a mobile node gets compromised by attacker to perform such malicious activities. To address this security related problems, researchers introduced different methods to detect and the prevent this attacks in MANET. The recent methods like TWOACK, 2ACK, DSR, EAACK etc. proposed for misbehaving nodes detection and prevention with the goal of enhancing the network performance metrics in presence of attackers in network. However, such methods performing efficiently against the attacks like collaborative attacks in which group attacks comes together for common purpose and threatening the network. Therefore, to save impact of such attacks on individual mobile communications and information's, we need to have efficient technique to defend against different types of malicious nodes attack.

2.2 Proposed Solution

Therefore, in this paper to improve the performance of recent CBDS method, we modified this method with proposed approach disjoint path communication approach. The Trust Based Multi-Path Routing algorithm provides multiple disjoint paths from source to destination while providing security against different network attacks with goal of reducing the traffic load and hence end to end delay. Hop count of all nodes is considered from destination. In this scheme from source, only one path from each node is considered which is one hop away and is having hop count less than that of the source node. The recent reporting rate is separated by the many upstream neighboring nodes of the source and this new reporting rate is allocated over the each and every path. The node will get the packet and forward it only if it is from that dedicated path, else it will discard that packet. This process will be carried till packet reaches to destination. Figure 1 is showing the system architecture with existing and proposed approach adopted for practical work analysis.

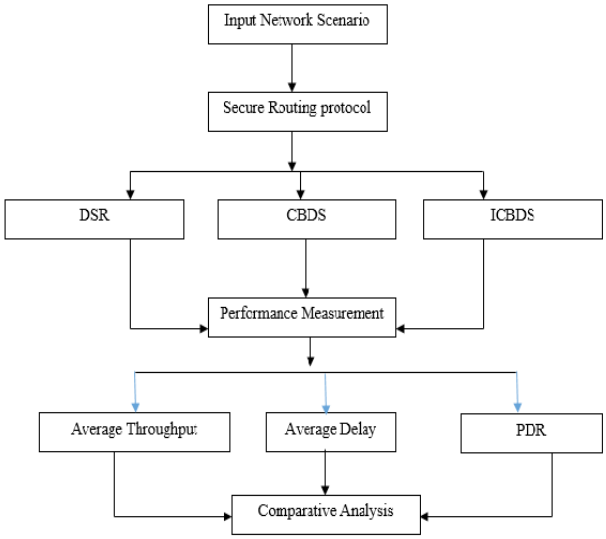

Figure 1. Proposed framework malicious nodes attack in MANET.

2.3 Algorithm Design

Here we formed ICBDS scheme by combining the CBDS algorithm with proposed disjoint path algorithm. Therefore, first we are presenting algorithm 1 for CBDS scheme, and then algorithm 2 for disjoint path scheme:

Algorithm 1: CBDS

Step 1: Source node start sending RREQ packets for route discovery

Step 2: If source received route reply within time, it means destination node is true destination, and then start forwarding data to it.

Step 3: else if current time is greater than discovery time threshold value, then current time is stored into T1

Step 4: else start resending the RREQ packets, measuring another threshold value of time in T2.

Step 5: Compute the current communication PDR performance

PDR = no_recieved/no_sent;

Step 6: Set threshold = 0.9;

Step 7: if (PDR < threshold), sending bait RREQ

Step 8: Update dynamic threshold value

Step 9: if (T2<T1), then

if (threshold < 0.95), then

threshold = threshold + 0.01;

else

if (threshold > 0.85), then

threshold = threshold - 0.01;

Step 10: if (Time < 800), then

return threshold;
else
threshold = 0.9;
Step 11: Stop

Algorithm 2: Disjoint Path Communication
Step 1: Find all available disjoint paths from source to sink through routing protocol.
Step 2: Consider hop count of all nodes from sink.
Step 3: Source node calculates its upstream nodes (say n) and keeps only one path from each node towards destination.
Step 4: Calculate New Source Initiated Bulged Reporting Rate by dividing current RR by neighboring nodes of source and then assign new RR to each path.
Step 5: If received packet is
i) from higher Hop count node and
ii) from the path of which the current node is member
Then accept and forward the packet.
Step 6: Else drop the packet.
Step 7: Repeat step 5 and 6 till packet reaches the destination.

3. Results and Discussion

3.1 Simulation Environment

For the simulation work we need a following setup for the technical work

1) Cygwin: for the windows XP, 2) Ns-allinone-2.32. There number scenario and the traffic files wants to generate in order to evaluate the performance of the routing protocols into the various network conditions. In this simulation the main parameter which is varied during the simulation is the number of nodes, number of connections and size of the network. Following are parameters which are varied for these simulations and depicted in Table 1.

Table 1. Simulation configuration

Number of Nodes	50
Traffic Patterns	CBR (Constant Bit Rate)
Network Size (X * Y)	1000 x 1000
Max Speed	10 m/s
Simulation Time	50s
Transmission Packet Rate	10 m/s
Pause Time	1.0s
Routing Protocol	DSR/CBDS/ICBDS
MAC Protocol	802.11
MAC Protocol	802.11
Channel Data Rate	11 Mbps
Number of Malicious Nodes	0 %-40 %

3.2 Simulation Results

We have compared the performance of three routing protocols using three performance metrics such as DSR, CBDS and proposed ICBDS technique. The results in Figures 2, 3 and 4 are showing that performance of proposed ICBDS approach against existing methods for security against malicious nodes in MANET. From these results it is showing that ICBDS is improving the performance as compared to CBDS method in terms of PDR, throughput and most importantly end to end delay. CBDS method is having drawback of poor end to end delay performance as compared to DSR method, which is overcome by proposed ICBDS here in above results.

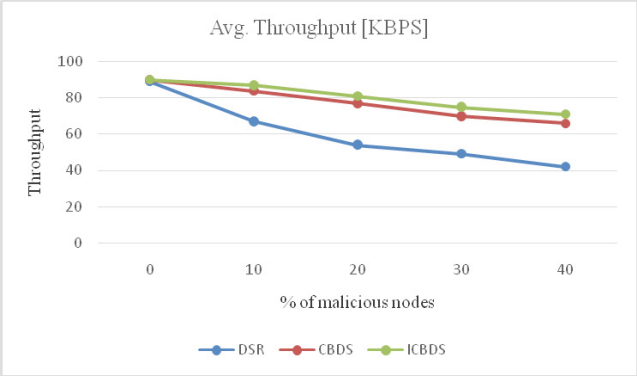

Figure 2. Average throughput analysis for different security methods of MANET.

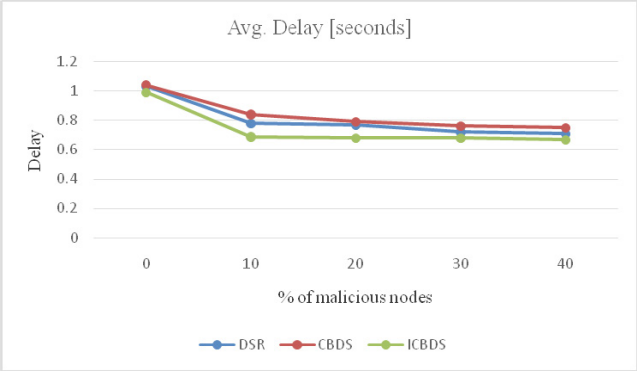

Figure 3. Average throughput analysis for different security methods of MANET.

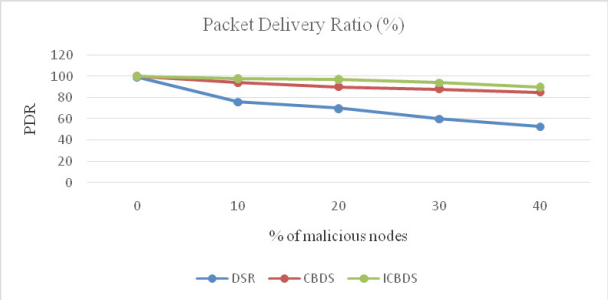

Figure 4. PDR analysis for different security methods of MANET.

4. Conclusion and Future Work

For MANET, security is important research challenge in order to defend against malicious, selfish, and gray hole attacks. In this paper, we proposed the approach for defending against the collaborative malicious node attack in MANET using improved CBDS method called ICBDS. ICBDS is based on existing CBDS method by adding multiple disjoint path communication. This paper shows the algorithm design, simulation parameters and expected results for three important performance metrics such as average throughput, average end to end delay and packet delivery ratio. Our expected results are showing that proposed ICBDS method outperforming previous DSR and CBDS methods. For future work, we will apply this method on simulation environment and get more complex network scenarios for results analysis. Another future direction is uses of efficient cryptography will helps to secure the data communication.

5. References

1. Elhadi M, Shakshuki S, Kang N, Tarek R, Sheltami S. EAACK- A secure intrusion-detection system for MANETs. IEEE Transactions on Industrial Electronics. 2013; 60(3):1089–98.
2. Liu K, Deng J, Varshney PK, Balakrishnan K. An acknowledgment-based approach for the detection of routing misbehaviour in MANETs. IEEE Transactions on Mobile Computing. 2007; 6(5):536–50.
3. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehaviour in mobile adhoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA; 2000. p. 255–65.
4. Sheltami T, Al-Roubaiey A, Shakshuki E, Mahmoud A. Video transmission enhancement in presence of misbehaving nodes in MANETs. Multimedia Systems. 2009; 15(5):273–82 .
5. Liu K, Pramod D, Varshney K, Balakrishnan K. An acknowledgement based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing. 2007; 6(5):536–50 .
6. Xue Y, Nahrstedt K. Providing fault-tolerant ad hoc routing service in adversarial environments. Wireless Personal Communications. 2004; 29:367–88.
7. Baadache A, Belmehdi A. Avoiding blackhole and cooperative blackhole attacks in wireless adhoc networks. International Journal of Computer Science and Information Security. 2010; 7(1):1–5.
8. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehaviour in mobile adhoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, USA; 2000. p. 255–65.
9. Vishnu K, Paul J. Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks. International Journal of Computer Applications. 2010; 1(22):28–32 .
10. Kozma W, Lazos L. REAct: Resource-Efficient Accountability for node misbehavior in adhoc networks based on random audits. WiSec '09 Proceedings of the second ACM conference on Wireless network security; 2009. p. 103–10.
11. Wang W, Bhargava B, Linderman M . Defending against collaborative packet drop attacks on MANETs. Proceedings 28th IEEE International Symposium Reliable Distributed System. New Delhi, India; 2009 Sep. p. 1–6.
12. Chang JM. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. Systems Journal. 2014; 9(1):65–75.
13. Jabamani SS, Rajinikanth E. Integrity key based mechanism to debase packet dropping in MANETS. Indian Journal of Science and Technology. 2016 Apr; 9(14). DOI: 10.17485/ijst/2016/v9i14/90204.
14. Rajendiran M, Srivatsa SK. Route efficient on demand multicast routing protocol with stability link for MANETs. Indian Journal of Science and Technology. 2012 Jun; 5(6). DOI: 10.17485/ijst/2012/v5i6/30477.
15. Sahoo AJ, Akhtar MAK. Possibility and necessity measures to enhance reliability and cooperation in MANETS. Indian Journal of Science and Technology. 2014 Jan; 7(3). DOI: 10.17485/ijst/2014/v7i3/47650.
16. Sumathi A, Sundaram BV. An ANN approach in ensuring CIA triangle using an energy based secured protocol E-AODV for enhancing the performance in MANETS. Indian Journal of Science and Technology. 2015 Dec; 8(34). DOI: 10.17485/ijst/2015/v8i34/85243.
17. Rao M, Singh N. Performance evaluation of AODV nth BR routing protocol under varying node density and node mobility for MANETs. Indian Journal of Science and Technology. 2015 Aug; 8(17). DOI: 10.17485/ijst/2015/v8i17/70445.

18. Bai PTK, Sundararajan M. Performance efficiency of OLSR and AODV protocols in MANETS. Indian Journal of Science and Technology. 2015 Jul; 8(14). DOI: 10.17485/ijst/2015/v8i14/73048.