Credit Based Enhanced Routing Protocol for Early Identification of DDoS Attacks in MANETs

M. Savithri

{ Savithri.m@christuniversity.in }

Assistant Professor, Department of Data Science, Christ University, Lavasa, Pune

Abstract. The incorporation of competent trust mechanisms in mobile adhoc networks (MANET) has gained a lot of attraction during the past two decades, and numerous trust and security establishment solutions based on various cryptography and hashing technequies have been used. Although effective, these approaches generate large processing and communication overheads and use energy in MANET. The routing protocol is essential for effective communication between nodes and functions under the premise that nodes are completely cooperative. Some nodes may not collaborate properly because to the open structure and limited battery-based energy. Recently, approaches for enforcing collaboration have developed to establish a trust based approach in MANET. These methods, classed as reputation and credit based, are designed for networks with limited processor, battery, and memory resources, as well as where key or distribution of certificates through the centers are absent or ephemerally present. Alternatively, they contribute to the identification of peer trustworthiness and to enforcement cooperation through the use of reciprocal incentives. A Credit Based Enhanced Routing Protocol (CBERP) for MANET is suggested, which is an attack-resistant credit-based cooperation mechanism that deals with the selfish node's Distributed Denial of Service (DDoS). It provides good protection against selfish attacks in MANET routing systems.

Keywords: MANET, DDoS attack, Selfish node, Routing Protocols, TAODV and Security.

1 Introduction

MANETs have piqued the interest of both researchers and commercial developers because to their rapidly expanding range of capabilities and diverse applications. It appears conceivable that MANET nodes are independent entities that manage their own assets such as usage of available power in the battery and bandwidth of transmission [1]. The detracting value of MANET node is based on the availability of power in the battery and bandwidth capacity of the transmitting node is a key driver for not advancing messages from another nodes. This uncooperative conduct wreaks havoc on the complete performance of the network. To overcome node deficiency of teamwork, it is necessary to offer them with an inducement mechanism to behave cooperatively and advancing network packets. In wide-ranging, these strategies can be

IACIDS 2023, November 23-25, Lavasa, India

DOI 10.4108/eai.23-11-2023.2343239

divided into three categories: reputation-based mechanisms, credit-based mechanisms, and game-theoretic mechanisms, as shown in Figure 1. Reputation-based techniques [2,3,4] are based on observing the performance of the node from the perception of cooperation and isolating problematic nodes. This technique has numerous serious flaws [5]. The first is that formal evaluation of these mechanisms is not conceivable. The second fault is the formation of a group of nodes who are conspiring to enhance their utility. The third flaw in this technique is its reliance on wireless networks' broadcast nature [6].

The second type of collaboration mechanism employs credits in the form of micropayments [7]. Each node is compensated for its participation in passing network communications and also compensates supplementary nodes that participate in promoting its messages. As a result, nodes can advancing messages using credits earned from other nodes. All of the payments described above are micropayments. Credit-based mechanisms outmaneuver reputation-based processes for node cooperation. The threat of dishonest node behavior threatens credit-based processes. Early efforts are made to eliminate the behavior [3, 9] developed systems in which tamper-proof hardware ensures payment security issues.

The third type of cooperation mechanism is the game theoretic mechanism, which attempts to avoid retaliatory situations if a node is mistakenly regarded as selfish in order to quickly restore cooperation. One of the primary disadvantages of this mechanism in MANET is that they all assumed perfect observation and most of them did not consider the effect of noise on strategy creation. However, in this network, even if a node decides to forward a packet for another node, the packet may be missed owing to link failure or transmission faults. Fig 1 represents the cooperation mechanisms used in MANET.

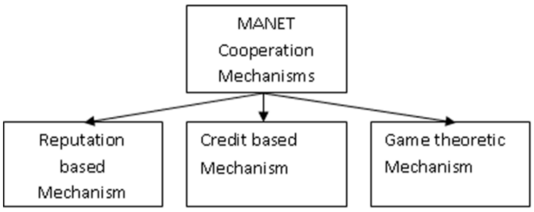

Fig. 1. The Taxonomy of Cooperation mechanism models for MANET

In the remaining section of this paper is organised such that Section II will provide the details of previous works that supports the node cooperation mechanism in MANET. Scheme Description and Methodology are covered in Section III while the Section IV describes the CBERP protocol design. Section V discusses the analytical examination of CBERP. Section VI depicts the simulation scenarios and results. Section VII has some final observations, while Section VIII provide the conclusion.

2 Related Works

Recent research efforts have concentrated on protecting MANETs, with the majority aimed at securing routing protocols. Authentication and network node cooperation are the two most important security issues in MANET. Authentication is essentially a procedure by which two parties identify one another. Without authentication, an unauthorised node might easily "come in" and access the network's resources. The situation is exacerbated if the unauthorised node is malevolent. As a result, a technique for prohibiting a "outsider" from joining the network is required. Previous work [14] suggested an authentication system called Efficient Secure nhanced Routing system, which is an attack resistant authentication mechanism. An detailed examination of the ESERP protocol in MANET was undertaken in this work to provide a more secure data transmission method against protocol attacks than the existing protocols. ESERP has solved the authentication problem. The disadvantage of this protocol is that the network node's cooperative behavior is not examined. As a result, this work agreement will fascinate the cooperation problem in the MANET. An overview of relevant works in MANET security, with a focus on the credit-based system aimed at protecting against DDoS attack.

Zhong et al. [5] presented SPRITE, which is an incentive-based system where the selfish nodes in the network are been motivated and converted it into a cooperative node. The node will send a message to the Credit Clearance Service (CCS) center the details about the received and forwarded packets. When an intermediate node forwards a message from another node, it gains credit. Sprite presupposes source routing and a public key architecturealong with the existence of the central authority. It also employs the concept of digital signature for every transactions. CCS is expected to be reachable via the internet in SPRITE's network design, limiting the utility of the sprite.

A wireless health monitoring based system is been proposed such that it uses incentive based route collaboration in [14]. For enhancing message delivery reliability, it employs two co-operation protocols: Continuous Value Cooperation Protocol (CVCP) and Discrete Value Co-operation Protocol (DVCP). The CVCP protocol validates the value of offered and saved credits. DVCP is intended for smaller adhoc networks and employs approximations such as high (H), medium (M), and low (L) to represent the incentive. Credits are assigned based on the priority of the message.

Prioritiztion in forwarding is introduced in [15] to provide incentives based on the collaboration provided by the nodes in forwarding the packets in the network. An adhoc network in this system serves two sorts of traffic based on the nodes that put good effort in forwarding and priority. For forwarding the packets if the source node is paying then the priority is given for the packet in the network by the intermediate nodes in transferring the packet to the intermediate nodes and also transfer the credit else the best effort service is offered. The downside of this strategy is that it presupposes that every node in the network will give best effort service, which is not guaranteed. It does not handle concerns such as tracking the currency of other nodes in the network, correlations between different greed measurements, node behavior, and the resulting system's equilibrium.

3 Possibility Of DDoS Attack

A Distributed Denial of Service (DDoS) attack is been implement in a large-scale in mobile adhoc network to reduce the availability of resources in the network. The DDoS assault is initiated by simultaneously send an extraordinarily large amount of packets to a goal system with the collaboration of a great number of hosts scattered all over the Internet. Network bandwidth of the nodes in the network are been consumed by the attackers by targeting the host node and sending genuine requests that might be rejected. The consequences of these attacks can range from slight irritation to website visitors to significant financial losses to businesses that depend on the availability of the business conduct.

DDoS assaults are projected to become a growing threat to the Internet as a result of the widespread availability of user-friendly attack tools that aid in the coordination and execution of large-scale DDoS operations. With the help of these tools, even inexperienced users may launch a devastating onslaught. Tools such as Trinoo, TFN, TFN2K, Shaft, and Stacheldraht are available and have been used in DDoS attacks on recognised commercial websites such as Yahoo, Amazon, and Ebay. The only method to totally eradicate the DDoS threat is to safeguard all Internet-connected equipment beside misuse, which is impractical. Most large websites currently deal with the issue by providing ample resources to important systems.

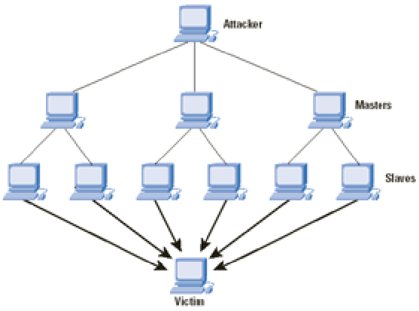

Fig 2. DDOS Attack

Recent advancements in DDoS protection systems have effectively ended the age in which script-kiddies could download a tool and conduct an assault against nearly any website. Attackers employ increasingly advanced tactics to initiate DDoS attacks today. Despite all efforts to reduce the number of DDoS attack occurrences, the frequency and size of the targeted networks and machines have grown dramatically.

4 System Design and Methodology

Credit Based Enhanced Routing Protocol (CBERP) is an attack-resistant incentive protocol that protects MANET routing protocols from selfish attacks. It detects node non-cooperation, assisting nodes in dropping faulty packets sooner by finding the malicious node immediately. This form of attack depletes server resources or those of transitional communication equipment like firewalls and load balancers. CBERP handles data traffic and traffic control assaults. This attack classification is created on their collective qualities and attack objectives. For example, the Black Hole attack drops packets each time, but the Gray Hole assault drops packets based on dual conditions: time or dispatcher node.

The suggested procedure includes the following steps:

- Source should is authenticated by the terminus node

- All the middle nodes that are listed in the header of the packets are been authenticated by the terminus node

- The sequence and the correctness of the nodes in the list is been confirmed by both the source and the destination node.

- Hop-by-hop signatures provide effective security against protocol assaults.

Before communicating the data to the destination node, the dispatcher node will generate a temporary pair of key under the suggested protocol. The key pair is made up of a secret key list SS and a public key PS. It generates the secret key lists SS0, SS1 using the one-way hash function approach. The public key PS can be generated by hashing each entry of the list SS1.

5 Protocol Design of CBERP

Each network node keeps an supplementary data structure called the Neighbour's Trust Counter Table (NTCT). The NTCT solves the challenges associated with secure routing by employing trust counters in a credit-based incentive mechanism. Let TCC1, TCC2,... represent the preliminary confidence counters of the nodes N1, N2,... in the path from a source S to a destination D.

Because the node has no evidence about the dependability of its neighbors from the start, nodes can neither be entirely reliable nor fully distrusted. When a source S wishes to deliver a packet to a destination D, route request (RREQ) packets are sent. Using a trusted credit counter (TCC), each node maintains trajectory of the amount of packets delivered across a route. Attacks on transmission tables are detected utilizing a credit-based incentive scheme and a trustworthy credit value counter. When node Nk receives a packet from node Ni, Nk increments the credit counter of node Ni

$$TCCNi = TCCNi + 1, \; i = 1, 2\ldots\ldots \qquad (1)$$

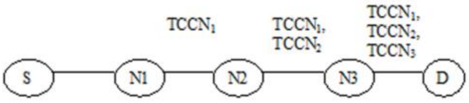

Fig 3. Incentive Scheme

6 Performance Evaluation

Both Analytical and simulation model are used to evaluate the enactment of the proposed model. The analytical model is mainly used to compute the end to end delay of the packet that are been transmitted. While NS2 is used to simulate the proposed model. The channel capacity of the simulation of the mobile host is been set to 2 Mbps and 100 nodes are been used for the simulation with 1000 X 1000 meter square region and the time for simulation is set to 50 seconds. It is been considered that all the nodes have the same transmission range.

There are various performance metrics that are involved but based on the problem definition the performance metrics that has been selected for the evaluation are Control Overhead, Average end-to-end delay, Average Packet Delivery Ratio, and Packet Loss Ratio.

7 Simulation and Results

The proposed CBERP protocol is compared to the existing TAODV (Trusted AODV) protocol. The existing protocol TAODV has several notable features, including: (1) Nodes accomplish trusted routing behaviors primarily based on the trust relationships between them; (2)A node that engages in malicious behavior will ultimately be detected and denied access to the entire network; and (3)System performance is enhanced by avoiding the generation and verification of digital signatures at each routing hop. In our experiment, the number of attackers is varied as 5, 10, 15, 20, and 25.

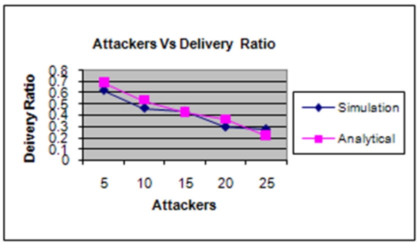

Fig 4. Attackers Vs Delivery Ratio

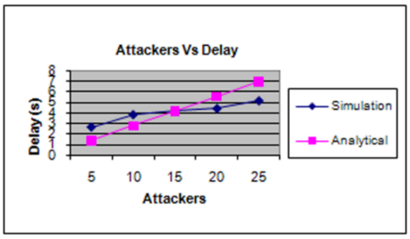

Fig 5. Attackers Vs Delay

Figure 4 depicts the packet delivery ratio results for the disobedient nodes 5, 10,....25 in the 100 node state. The analytical and simulation findings converge with a 10-20% discrepancy. As the number of assailants increases, so does the delivery ratio. Figure 5 depicts the delay results for the disobedient nodes 5, 10,....25 in the 100 node state. We can see that the analytical and simulation findings converge with a 20-30% discrepancy. As the number of assailants grows, so does the delay.

7 Conclusion

The development and testing of a Credit Based Enhanced Routing Protocol (CBERP), a novel mobile adhoc network routing protocol that provides secure routing and improved node cooperation in MANETs. The TAODV routing protocol is used in the design. The mechanisms based on reputation and those based on game theory are compared. CBERP assists nodes in dropping incorrect packets earlier by immediately spotting malicious nodes by checking the digital signatures of all transitional nodes. It punishes bad nodes by decrementing a trusted credit counter and compensates good nodes by increasing the credit counter. As a result, uncompromised nodes are prevented from assaulting routes with malicious or compromised nodes. The suggested protocol CBERP has an overall performance of 75-80% compared to the existing protocol TAODV, which has an overall performance of 55-65% (based on the two scenarios). Attackers and pause time are the first two things to consider. The proposed protocol focuses on efficient data traffic and control traffic security in MANET. For energy-constrained mobile nodes, the computational overhead is measured. CBERP demonstrates the existing protocol's efficiency in providing a secure data transfer path against Protocol assaults in MANET.

References

[1] M. Velayanikal, 13 January 2018. [Online]. Available: https://www.business-standard.com/article/economy-policy/bhim-app-market-share-falls-to-6-as-tez-phonepe-and-paytm-make-gains-118010500063_1.html.

[2] Statistics, 8 March 2018. [Online]. Available: http://rbidocs.rbi.org.in/ rdocs/content/ docs/ELECT07022016_A.xls

[3] Product Overview, 2016. [Online]. Available: https://www.npci.org.in/product-overview/upi-product-overview.

[4] Digital payments in India to reach $1 trillion by 2023: Credit Suisse,“ 15 February 2018. [Online]. Available: https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/digital-payments-in-india-to-reach-1-trillion-by-2023-credit-suisse/articleshow/62935890.cms

[5] D. S. Denis Dennehy, Trends in Mobile Payments Research : A Literature Review,March 2015. [Online]. Available: https://www.researchgate.net/publication/275155059.

[6] X. Song, „Mobile Payment and Security,“ rev. Seminar on Network Security, 2001

[7] K. P. a. K. T. Nina Kreyer, „Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce,“ Munich Personal RePEc Archive, 2002

[8] D. J. K. Basudeo Singh, „Enabling P2P Mobile Payment through P2P Network,“ IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), 2012

[9] N. M. Tomi Dahlberg, MOBILE PAYMENT SERVICE DEVELOPMENT – MANAGERIAL IMPLICATIONS OF CONSUMER VALUE PERCEPTIONS, ECIS, 2002

[10] B. N. a. S. Sun, „Using Text Mining Techniques to Identify Research Trends: A Case Study of Design Research,“ MDPI, 2017

[11] M. K. H. S. A. a. F. F. Ramzan Talib, „Text Mining: Techniques, Applications and Issues,“ (IJACSA) International Journal of Advanced Computer Science and Applications, 2016

[12] A. K. a. S. Naithani, „A Comprehensive Study of Text Mining Approach,“ IJCSNS International Journal of Computer Science and Network Security, 2016.

[13] D. K. a. J. W. Kim, „Public Opinion Mining on Social Media: A Case Study of Twitter Opinion on Nuclear Power,“ Advanced Science and Technology Letters , 2014

[14] M. Mulins, „Information extraction in text mining,“ Computer Science Graduate and Undergraduate Student Scholarship, 2008

[15] S. R.Sagayam, „A Survey of Text Mining: Retrieval, Extraction and Indexing Techniques,“ International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5, 2012