International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195275

Secured Routing in Mobile Ad hoc Networks (MANETs)

S. Maharaja, R. Jeyalakshmi, A.V. Sabarish Kanna, M. Deva Priya
Department of Computer Science & Engineering, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

A Mobile Adhoc Network (MANET) is prone to attacks. Adversaries take hold of the network, thus degrading their performance. Various attacks are prevalent in MANET, out of which Byzantine attack plays a vital role. A node or group of nodes present in the routing path between the source and the destination may be compromised due to Byzantine attack. In this paper, Cohen Kappa Reliability Coefficient based Mitigation (CKRCM) mechanism is proposed to deal with these attacks. The intermediate nodes are monitored by their neighbors for a timestamp. If the monitoring node does not receive an acknowledgment, then the nodes are perceived to be attacked. The trustworthiness of the nodes is built by computing the trusts and reliabilities of the nodes. It is seen that the proposed scheme outperforms the existing scheme in terms of Throughput, Packet Delivery Ratio (PDR) and Packet Loss Ratio (PLR).

Keywords : MANET, Byzantine Attack, Cohen Kappa Reliability Coefficient, Trust Factor, Reliability

I. INTRODUCTION

The latest growth in wireless communication drives the users towards the vigorously growing technology - mobile communication. The use of laptops, wireless modems and wireless Local area Networks (LANs) that are available at a lower cost with higher data rate are the main reasons for such a rapid evolution. As these devices are lightweight and portable, the mobile users find them convenient to carry. People prefer wireless communication networks rather than the conventional wired equivalents, as they offer endless connections.

1.1 Adhoc Networks

In contrast to the infrastructure networks, ad hoc networks do not include Base Stations (BSs). They assist in anytime/anywhere computing by supporting wireless communication between devices with networking capabilities. It is a Local Area Network (LAN) that does not depend on a preexisting infrastructure, and hence can be dynamically created and maintained. The networks take control of message transmissions as all the nodes forward packets between them not relying on the BS. The nodes may be arranged in either of the two main topologies namely, heterogeneous and homogeneous/ fully symmetric.

- ✓ **Heterogeneous** - The nodes possess different capabilities.
- ✓ **Homogeneous or fully symmetric** - The nodes have identical capabilities and responsibilities.

1.2 Mobile Ad Hoc Network

The various sectors in the field of wireless communication include cellular telephony, satellite-based communication and Wireless Local Area Networks (WLANs).

There are two different categories that are described by the IEEE 802.11 standard of wireless networks for WLANs built on the structure namely, infrastructure-based and infrastructure-less (ad hoc) networks. APs establish communication between the mobile nodes and wired networks [1].

Basic Service Set (BSS) [2] is a set of mobile nodes that are associated with a specific AP. To enhance the Wi-Fi range, a number of BSSs may be connected with a distribution system called Extended Service Set (ESS). A common Service Set Identifier (SSI) is assigned to all APs in the ESS which acts as the network.

An efficient choice to exchange data without any fixed infrastructure is offered by ad hoc WLANS. To create an Independent Basic Service Set (IBSS), the mobile nodes have to collaborate into a peer-to-peer network [3].

Every mobile node that forwards packets to foreseen destinations requires a routing mechanism [4]. In Mobile Ad Hoc Network (MANET), the mobile nodes act as routers, thus forming a backbone of the dynamic network and extending the range of ad hoc WLAN [5]. In MANET, the nodes cooperate with each other and act as relays to implement diverse operations like security and routing. They do not demand any centralized control for monitoring events. Selfish nodes in the network either postpone or drop the packets.

II. ROUTING

The topology changes are frequent and unpredictable due to the dynamic nature of the nodes, thus leading to an increase in the routing overhead. Routing is an uphill task as finding an efficient path to the destination depends on various factors like Residual Energy (RE), Received Signal Strength (RSS) of the next hop node, topology, location of the request initiator and so on. Routing is an important area that demands much attention. There are a number of routing protocols available in the literature. They are broadly classified into the following.

- ✓ Topology based approach
- ✓ Location based approach
- ✓ Power/energy aware approach

2.1 Topology based approach

In topology based approach, each mobile node relies on its knowledge about the status of latest connectivity and state of network links [6]. Based on the time of discovery and updation of the routes, the routing protocols are classified into the following:

- ✓ Proactive Routing Protocols
- ✓ Reactive Routing Protocols
- ✓ Hybrid Routing Protocols

Proactive Routing Protocols

In Proactive protocols, the routing information is maintained in tables, hence known as “table driven” protocols. The nodes find the path to all the nodes by storing updated and consistent information in the routing table. This enables the source node to find the routing path immediately whenever required. The nodes send route updates for route creation and maintenance periodically [7].

The routing updates occur at specific intervals. In case of event-triggered updation, updates are done whenever there are some changes in the network. Increase in mobility rate directly leads to increase in the rate of updates. The nodes are aware of the routes to all the nodes in the network, and hence it is possible to find the routes at any instant of time. However, there is an increase in the control overhead with event-triggered updates as the mobility rate has a direct impact on the rate of updates. Some proactive routing protocols in MANET include Wireless Routing Protocol (WRP), Destination Sequence

Distance Vector (DSDV) and Fisheye State Routing (FSR).

Reactive Routing Protocols

As the nodes in reactive routing protocols do not maintain a route to other nodes, they are known as "on-demand routing" protocols. A path to a node is found only on need.

In proactive protocols, the control overhead is high as more updates are required with the frequent changes in link connectivity. On the other hand, in reactive routing protocols, the routes are discovered only when needed. A node checks the routing table to know whether a route exists when it wants to communicate with another node. A route discovery procedure is invoked on-demand.

In the route discovery phase, Route-REQuest (RREQ) packets are forwarded by a node to all its neighbor nodes, until it reaches the destination. The destination responds by forwarding a unicast Route-REPly (RREP) to the source. The route establishment phase is followed by route maintenance [8].
Some reactive routing protocols in MANET include Dynamic Source Routing (DSR) [9] protocol, Ad hoc On-demand Distance Vector (AODV) [10] protocol and Temporally Ordered Routing Algorithm (TORA) [11].

Hybrid Routing Protocols

Hybrid routing protocols are a blend of both proactive and reactive protocols. Zone Routing Protocol (ZRP) [12] is the best example.

2.2 Location based approach

Routing involves the geographic position of nodes obtained using GPS. Location-Aided Routing (LAR) [13] is the best example for location based routing protocols. The RREQ packets are forwarded to a small group of nodes based on the location of the destination.

During the route discovery phase, the RREQ packets including the location information of both the source and the destination are forwarded to all the nodes within the request zone. The nodes in the request zone forward the message, while the others discard. The RREP includes the current location of the destination. If the route to the destination cannot be found, then the routing messages are flooded throughout the network.

2.3 Power or Energy Aware Approach

COMmonPOWer (COMPOW) is an energy aware protocol wherein, for each power level, a routing table is maintained on the wireless card. Hello messages are exchanged at each power level, and the tables are built [14]. The number of entries in the routing table of a node depends on the number of nodes that are reachable from it at a power level. The last entry in the routing table gives the total number of nodes that can be reached at maximum power. The master routing table is found once the optimal power level is computed.

III. SECURITY ATTACKS IN MANET

The dynamic nature and structure of MANETs has led to a variety of highly vulnerable attacks. The fundamental need for a secured networking is secure protocols that confirm secrecy, accessibility, authenticity and reliability of the network. Most of the prevailing security solutions for MANET setting are not effective and efficient. Since the transmission is in an exposed scenario, there is a high probability of attacks. The attacks can be highly reduced if a security protocol is deployed. The association of intricate mobile nodes determines the success of MANETs as it spontaneously institutes paths among one another for communication.

3.1 Classification of Security Attacks

Attacks may be categorized based on the behavior of the attack i.e. Passive or Active attack.

✓ **Passive attacks:** In the case of passive attacks, the data transmitted within the network is not altered. But it involves unauthorized "listening" to the network traffic or accumulation of data from it. It does not disrupt the operation of a routing protocol but attempts to discover important information from the routed traffic.

✓ **Active attacks:** Active attacks can be either internal or external, hindering the message flow between the nodes. Active external attacks are initiated by outside sources that do not belong to the network. Internal attacks are from malicious nodes that are a part of the network and are hard to detect when compared to the external attacks. These attacks support unauthorized access in the network letting the attacker to make changes such as modification of packets, DoS, congestion etc.

IV. BYZANTINE ATTACKS

Byzantine problem refers to the situations where a few defective members of the group show an arbitrary behaviour and lead to system malfunction [16]. This kind of problem was first stated by Lamport (1982) [17] as "Byzantine General Problem". In the case of Byzantine attacks, the adversaries take control of the authenticated devices and show arbitrary behavior that disrupts the network [15]. Once the attackers make the active set of nodes malicious, the whole network comes under the dominion of the adversaries, thus disrupting secured data transmission. This attack has a diverse effect in military and medical applications. An adversary may prevent route establishment by dropping the RREQs and RREPs, modify the route selection metrics such as packet IDs and hop counts, selectively drop packets, create routing loops, forward packets through non-optimal paths consuming more time and bandwidth and so on. It results in disruption or degradation of the routing services and network performance. If the packets in critical applications are modified by an adversary, it will mislead the receivers and may cause the receivers to make wrong decisions.

Selfish nodes do not take part in the routing and do not spend their own resources. On the other hand, a byzantine node interrupts the communication of other nodes in the network, without considering their own resource utilization. There are diverse forms of Byzantine attacks like black hole or sinkhole attacks, byzantine wormhole attacks, byzantine overlay network wormhole attacks, gray hole attacks, flood rushing attacks and selfish node attacks.

V. RELATED WORK

The works done by various authors to handle Byzantine attacks are discussed below.

Perlman 1988 [18] has carried out a study on Byzantine attacks in the networking layer, which incurs more networking cost and processing overhead. Two approaches are presented - one based on a flooding algorithm for path discovery and the other based on link state method.

To ensure security, Swarm Intelligence paradigm and Distributed Reinforcement Learning are used by Awerbuch et al (2003) [19]. The source routes the actual data packets and the reliability of the packets is ensured by reverse ordered Hash Message Authentication Code (HMAC) technique. The source entrusts the responsibility of forwarding packets and returning acknowledgments to the nodes by maintaining a graph and the probabilities of reaching destinations. The probability distribution is dynamically determined. The intermediary nodes are not allowed to make hop by hop routing decisions.

Awerbuch et al (2005) [20] have evaluated the stationary state performance of the On-Demand Secure Byzantine. Resilient Routing (ODSBR) Protocol and have analyzed several Byzantine node attack models. The attack models include both non-

colluding and colluding nodes in MANET. The ability of ad hoc routing protocols to withstand failures and Byzantine attacks is analyzed.

Vempaty et al (2013) [21] have used Byzantine attacks for location estimation in Wireless Sensor Networks (WSNs) using binary quantized data. They have used Posterior Cramér-Rao Lower Bound (PCRLB) to characterize the performance of the network.

Kailkhura et al (2013) [22] have dealt with the problem of finding the optimal fusion rule under the constraint of fixed local sensor thresholds. Fixed Byzantine strategy is considered. Next, the problem of joint optimization of the fusion rule and local sensor thresholds for a fixed Byzantine strategy is studied. These results are applied to the scenario where both the Fusion Centre (FC) and the Byzantine attacker act in a strategic manner.

5.1 Intrusion Detection System

Han et al (2007) [23] have proposed LASIRC, an authentication-free, gossip-based application-level propagation mechanism, wherein Byzantine features are used to defend the nodes from Byzantine attacks. It is robust to message-denying, message-faking attacks and Black Hole Class (BHC) attacks.

A mathematical framework for determining the performance bounds of Byzantine attackers and the Intrusion Detection System (IDS) in terms of detection delay is proposed by Baras et al (2007) [24]. The problem of distributed collaborative defense against coordinated attacks in MANETs is addressed as a dynamic game problem. A collection of attackers observe the network and provide versatile support to the attack. In addition, groups of defending nodes synergistically examine the network and synchronize their actions against the assailants. A mathematical framework for efficient identification of attacks and damages is provided. Sequential Probability Ratio Test (SPRT) is used to detect the attacks. In addition, a voting mechanism is presented to improve the consistency of the IDS against malicious users who try to undermine the verdict of the IDS.

In case a Byzantine attack is detected, the nodes that have launched the attack are to be isolated from the network, so as to avoid the intricacy of error rectification and acceleration of the attack. According to the framework proposed by Jafarisiavoshani et al (2007) [25], under randomized network coding, the information about the topology is given by the subspaces at the nodes. In case of a single adversary, atmost two nodes are identified with uncertainty. Using subspace network error correcting codes, a coding vector is appended to each transmitted packet, and intermediate nodes perform randomized network coding.

5.2 Cognitive Radio Based Methodologies

Cognitive Radio (CR) has emerged as a solution to the problem of spectrum scarcity as it exploits transmission opportunities in the under-utilized spectrum bands of primary users. El-Hajj et al (2011) [26] have analyzed the performance limits of collaborative spectrum sensing under Byzantine attacks, where malicious users send false sensing data to the FC leading to increased probability of incorrect sensing results. In this approach, the FC identifies the attackers and removes them from the data fusion process.

Though the operational aspects of CR are explored to a greater extent, the security aspects have gained little attention. Kailkhura et al (2013) [22] have discussed briefly about CR technology followed by a detailed analysis of security attacks targeting Cognitive Radio Networks (CRNs) and few mitigation techniques.

He et al (2013) [27] have used the Markovian model for the spectrum state with Conditional Frequency Check (CFC) statistics. The collaborative spectrum

sensing performance is improved significantly with the assistance of one trusted user.

Collaborative spectrum sensing (CSS) enables secondary users in CRNs to collaboratively explore spectrum holes as well as protecting the primary users from being interfered. Bayesian learning is used by Nie et al (2017) [28] to design Byzantine defense schemes.

5.3 Secured Routing Protocol for Byzantine Attacks

Castro et al (2002) [29] have proposed a scheme in which routing is performed along multiple routes, so as to overcome Byzantine attacks. Redundant routing is expensive. Iterative routing imposes difficulty in verifying the correctness of each consecutive step. The iterative protocols proposed by Castro et al use cryptographic techniques for verification. Bogus requests that consume network resources are not considered.

Awerbuch et al 2002 [30] have propounded ODSBR routing protocol for MANETs. It is robust to outsider and Byzantine attacks. The source node has the knowledge of how other nodes in the network behave and has the capability to accurately monitor the behavior of nodes. It places a strict bound on the level of damage that a Byzantine node imposes on the network, independent of its behavior.

Avramopoulos et al (2004) [31] have presented a Byzantine Secure Link State Routing Protocol (BSLSRP) for wired environments. Technical feasibility is discussed in terms of processing overhead to evaluate the protocol over high speed data links.

Awerbuch et al (2006) [32] have extended his work in [20] by examining the progress of the learning algorithm proposed in the original ODSBR protocol, by analyzing new learning algorithms and exploring the effect of network layer and retransmission protocol on the resilience of the protocol. In addition to the Byzantine attack models, the dynamics of ODSBR against MAC-level attack is analyzed. An analytical model is designed to relate the learning time scales and the fundamental parameters describing the MANET and the protocol parameters.

The vulnerabilities of on-demand multicast routing protocols for multi-hop wireless networks are identified and the challenges encountered in overcoming them are discussed by Curtmola & Nita (2009) [33]. Byzantine-resilient Secure Multicast Routing (BSMR) uses reliability metric to mitigate Byzantine attacks for circumventing adversarial links.

A secure routing protocol to mitigate Byzantine Attacks is proposed for MANETs [32]. Secure Routing Against Collusion (SRAC) is designed in which each node takes the trust of its neighboring nodes and their performance to make a routing decision. Message and route redundancy during route discovery are involved in detecting internal attacks. To secure route-discovery messages, pairwise secret keys generated using public key cryptographic mechanisms are shared between the source and the destination along with some intermediate nodes along the route. A routing algorithm that builds a node's trustworthiness based on the behavior of the neighboring nodes is designed.

5.4 Distributed Detection of Byzantines

Chen et al (2008) [34] have discussed about distributed detection of cooperative Byzantine attack. It is assumed that a fraction of the monitoring sensors are compromised by an adversary. They are reprogramed to transmit false observations so as to confuse the decision maker at the Fusion Centre (FC). Measurements are made at the remote nodes.

Marana et al (2009) [35] have considered the problem of distributed detection in the presence of Byzantines under the Neyman-Pearson (NP) setup and determined the optimal attacking strategy so as to minimize the detection error exponent. This approach based on Kullback-Leibler Divergence

(KLD) is analytically tractable and yields approximate results in non-asymptotic cases.

Rawat et al (2011) [36] have analyzed the distributed detection of Byzantine attack in the context of CSS. They have assumed that the Byzantines determine the true hypotheses from their own sensing observations. The problem of distributed Bayesian detection in the presence of data falsifying Byzantines in the network is considered. The problem of distributed detection is formulated as a binary hypothesis test at the FC based on 1-bit data sent by the sensors. Chern-off information is adopted as the performance metric and the performance of the system under Byzantine attack in the asymptotic regime is studied. The expression for minimum attacking power required by the Byzantines to blind the FC is obtained.

Kailkhura et al (2013) [22] have dealt with the distributed detection of Byzantine attacks with independent identical sensors. The attacker is considered to be strategic in nature and a fusion rule with local sensor thresholds that minimizes the probability of error at the FC is designed. The problem of finding the optimal fusion rule under the constraint of fixed local sensor thresholds and fixed Byzantine strategy is considered. The strategic behavior of FC and the attacker are modeled using game theory and the existence of Nash Equilibrium is shown.

Distributed Spectrum Sensing (DSS) enables a CR network to reliably detect licensed users and avoid interference during licensed communications [37]. Incorrect spectrum sensing data are reported to a data collector which can lead to distortion of data fusion outputs. Various data fusion techniques focusing on their robustness against Byzantine failures are investigated. Weighted Sequential Probability Ratio Test (WSPRT) is introduced as a reputation-based mechanism to the Sequential Probability Ratio Test (SPRT).

The problem of distributed Bayesian detection in the presence of Byzantines in the network is dealt by Kailkhura et al (2015) [38]. It is assumed that a fraction of the nodes in the network are compromised and reprogrammed by an adversary and made to transmit false information to the FC. The problem of distributed detection is formulated as a binary hypothesis test at the FC and the expression for minimum attacking power required by the Byzantines to blind the FC is obtained. Existing asymptotic-based results do not hold under several non-asymptotic scenarios. When the fraction of Byzantines is not sufficient to blind the FC, a closed form expression is provided for the optimal attacking strategies of the Byzantines.

Hashlamoun et al (2017) [39] have considered the problem of distributed detection of Byzantines which seek to degrade detection performance by falsifying data. They have proposed a mechanism to partition sensors into groups to mitigate Byzantine attacks. The local decisions from the sensors in each group are sent to the FC via multiple paths.

VI. PROPOSED SYSTEM

In the proposed system, Byzantines in the network are eliminated by building the trustworthiness among the group of nodes during transmission. Routing loops are eradicated. The source establishes a reliable link to the neighboring nodes during mobility to reach the destination. The Route REQuest (RREQ) from the source is forwarded to the neighboring nodes. Some of the neighboring nodes send Route REsPonse (RREP) to the source.

The trustworthiness of a node say 'x' is based on the Trust Factor (TF). For instance, the probability that node 'x' will perform a particular action expected by a node 'y' is given by 'P_x^y'.

TF is calculated by analyzing the behavior of a node over a particular interval known as TF updating cycle. The actions include forwarding of RREQ, RREP, SMSG and data transmission. Each node maintains a Trust Certificate Repository (TFR). Based on the TF calculated, each node classifies its neighbors into three categories namely, known, unknown and companion.

- ✓ **Known** - Nodes with high probability of being trusted.
- ✓ **Unknown** - Nodes with low probability of being trusted
- ✓ **Companion** - Nodes with high probability of switching from unknown to known.

Let

'μ' - Probability that the link remains active and correct

- ✓ 'm_c'- Transmitted message found to be correct
- ✓ 'm_s' - Successful transmissions
- ✓ 'm_T' - Total number of messages transmitted by 'x' to 'y' which are not destined to 'y'
- ✓ 'm_A' - Total number of attempted transmissions

The trustworthiness of node 'y' by node 'x' is given by the following equation.

$$x(y) = \frac{mc+\mu ms}{mt+\mu ma} \quad (1)$$

Let

- ✓ '$T_{x(p;j)}$' - Trustworthiness on path 'p' by node 'x' on 'j^{th}' TF updation cycle.

The trustworthiness parameter stated above accounts for reliability, whereas availability of path also plays an important role in MANET as it has the inherent quality of link mobility. If 'H' is the number of hops in the path, 'V' is the average relative speed, 'R' is the transmission range,

where,

$$R = min(R_x) \quad (2)$$

'μ_0' - Constant of proportionality decided by node density and mobility scenarios

The parameter 'μ_{path}' is defined as shown in Equation (3),

$$\mu_{path} = \left(\frac{1}{\mu_0}\right)\left(\frac{H\ X\ V}{R}\right) \quad (3)$$

A Cohen Kappa Reliability Coefficient based Mitigation (CKRCM) mechanism for Byzantine attack in MANET is proposed. In this approach, the byzantine attack is detected through the following two steps

a) Identification of Routing loops.
b) Estimation of the reliability of mobile nodes

When the source desires to communicate with the destination, the source broadcasts the control packets through all possible paths. The probability of a node or group of nodes on the routing path between the source and the destination to get compromised by the Byzantine attack is high. Hence, the intermediate nodes are monitored by their neighbors for a timestamp (T_s). If the monitoring node does not get updates through acknowledgements, then it confirms that the node(s) is prone to attacks. Cohen Kappa Reliability Coefficient (CKRC) is computed.

Suppose a node 'N_a' is monitored by 'N_b' for identifying whether it is compromised and is a Byzantine. Then, the cumulative mean of probability (P_{FP}) that portrays the sustainability of nodes is given by Equation (4).

$$P_{FP} = P_{FP}^{a} * P_{BP}^{b} \quad (4)$$

Here,

The forward probability 'P_{FP}^{a}' estimated by neighbour 'N_b' on 'N_a' is computed as shown below.

$$P_{FP}^{a} = \frac{N_{FORW}^{a}}{N_{RECV}^{a}} \quad (5)$$

Similarly, the backward probability 'P_{BP}^{b}' estimated by neighbour 'N_a' on 'N_b' is computed as shown below.

$$P_{BP}^{b} = \frac{N_{FORW}^{b}}{N_{RECV}^{b}} \quad (6)$$

Suppose a node 'N_b' is monitored by 'N_a' for identifying whether it is compromised and is a Byzantine. Then, the cumulative mean of probability (P_{BP}) that portrays the sustainability of nodes is given by Equation (7).

$$P_{BP} = P_{BP}^{a} * P_{FP}^{b} \quad (7)$$

Here,

The forward probability 'P_{FP}^{b}' estimated by neighbour 'N_b' on 'N_a' is computed as shown below.

$$P_{FP}^{b} = \frac{N_{FORW}^{b}}{N_{RECV}^{b}} \quad (8)$$

Similarly, the backward probability 'P_{BP}^{a}' estimated by neighbour 'N_a' on 'N_b' is computed as shown below.

$$P_{BP}^{a} = \frac{N_{FORW}^{a}}{N_{RECV}^{a}} \quad (9)$$

where,

N_{FORW}^{a} , N_{FORW}^{b} - Maximum number of packets forwarded by nodes 'a' and 'b' respectively

N_{RECV}^{a} , N_{RECV}^{b} - Maximum number of packets received by nodes 'a' and 'b' respectively

Further,

The chance agreement Probability for the Expected reliability (P_{EP}) of the monitored node 'N_a'is given by Equation (10).

$$P_{EP} = P_{FP} * P_{BP} + (1 - P_{FP})(1 - P_{BP}) \quad (10)$$

Furthermore, the Observed Probability of 'N_a' by 'N_b'is given by Equation (11).

$$P_{OP} = P_{FP}\,(1 - P_{BP}) \quad (11)$$

Then, the Cohen Kappa Reliability Coefficient (CKRC) is computed as shown below.

$$CKRC = \frac{P_{OP} - P_{EP}}{1 - P_{EP}} \quad (12)$$

VII.RESULTS & DISCUSSION

Protocol-independent Byzantine-attack simulation module is developed using ns2. The Byzantine that forwards false information are identified in this module. Attacks like creating routing loops, selectively dropping packets and routing packets in non-optimal paths are carried out when a single or a group of malicious nodes work together. The intermediate nodes that are involved in such kind of attacks is found and circumvented. The performance evaluation based on Throughput, Overhead, Packet Delivery Ratio (PDR) and Packet Loss Ratio (PLR) with respect to number of nodes is shown below.

As the number of nodes increase, the throughput decreases negligibly as shown in Figure 1. Mechanism with CKRC offers 14.1% better Throughput in contrast to the mechanism not involving CKRC.

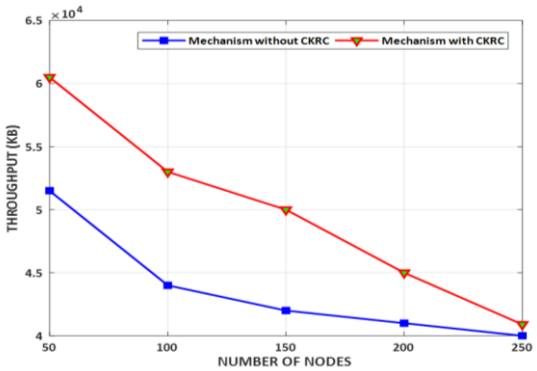

Fig. 1. Throughput

With increase in the number of nodes, the overhead slightly increases as shown in Figure 2. When compared to the mechanism without CKRC, mechanism with CKRC (CKRCM) involves 12.7% more overhead which is negligible.

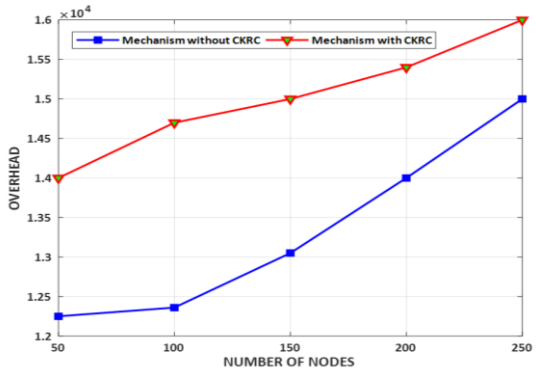

Fig. 2. Overhead

The Packet Delivery Ratio (PDR) decreases as the number of nodes are increased as shown in the Figure 3. Mechanism with CKRC (CKRCM) offers 16.1% better PDR in contrast to the mechanism without CKRC.

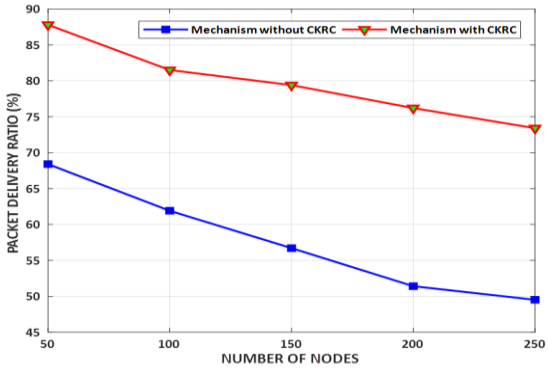

Fig. 3. Packet Delivery Ratio

As the number of nodes increases, the Packet Loss Ratio (PLR) increases as shown in the Figure 4. In contrast to the mechanism without CKRC, the mechanism with CKRC (CKRCM) involves 50% less PLR.

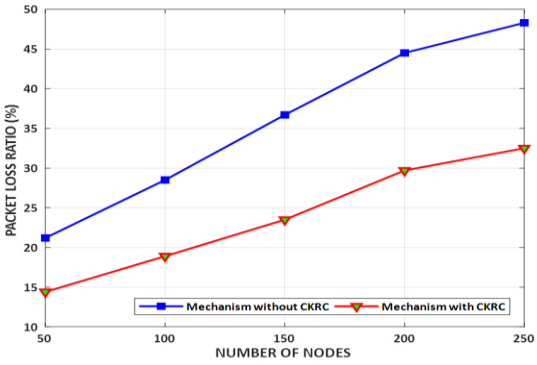

Fig. 4. Packet Loss Ratio

VIII. CONCLUSION

In this paper, a Cohen Kappa Reliability Coefficient based Mitigation Mechanism (CKRCM) was proposed to deal with the Byzantine attacks. The trustworthiness of the nodes was established to determine the steadfastness of the nodes. The mechanism is based on the expected and the observed probabilities of the nodes. CKRCM outperforms the scheme without Cohen Kappa Reliability Coefficient (CKRC) in terms of Throughput, Overhead, PDR and PLR.

IX. REFERENCES

[1]. Henry, P.S., & Lou, H. (2002). Wi-Fi: what's next, IEEE Communications Magazine, vol. 40, pp. 66-72.

[2]. Murthy, C. S. R., & Manoj, B. S. (2004). Ad hoc wireless networks: Architectures and protocols, portable documents. Pearson education.

[3]. Rauschert, P., Honarbacht, A., & Kummert, A. (2004, September). On the IEEE 802.11 IBSS and its timer synchronization function in multi-hop ad hoc networks. In Wireless Communication Systems, 2004, 1st International Symposium on (pp. 304-308). IEEE.

[4]. Perkins, C. E., & Bhagwat, P. (1994, October). Highly dynamic destination-sequenced

distance-vector routing (DSDV) for mobile computers. In ACM SIGCOMM computer communication review (Vol. 24, No. 4, pp. 234-244). ACM.

[5]. Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (Eds.). (2004). Mobile ad hoc networking. John Wiley & Sons.

[6]. Humayun Bakht, "Survey of Routing Protocols for Mobile Ad-hoc Network", International Journal of Information and Communication Technology Research, 2010-2011.

[7]. Royer, E. M., & Toh, C. K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. IEEE personal communications, 6(2), 46-55.

[8]. Kush, A., Taneja, S., & Sharma, D. (2010, December). Energy efficient Routing for MANET. In Methods and Models in Computer Science (ICM2CS), 2010 International Conference on (pp. 112-116). IEEE.

[9]. Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. Mobile computing, 153-181.

[10]. Mahdipour, E., Rahmani, A. M., & Aminian, E. (2009, March). Performance evaluation of destination-sequenced distance-vector (dsdv) routing protocol. In Future Networks, 2009 International Conference on (pp. 186-190). IEEE.

[11]. Park, V. D., Macker, J. P., & Corson, M. S. (1998, October). Applicability of the temporally-ordered routing algorithm for use in mobile tactical networks. In Military Communications Conference, 1998. MILCOM 98. Proceedings, IEEE (Vol. 2, pp. 426-430). IEEE.

[12]. Shafiq, Z., Mahmud, S. A., Khan, G. M., Sayyed, A., & Al-Raweshidy, H. S. (2012, October). Zone Routing Protocol: How does it perform the other way round?. In ICT Convergence (ICTC), 2012 International Conference on (pp. 71-77). IEEE.

[13]. Kush, A., Taneja, S., & Sharma, D. (2010, December). Energy efficient Routing for MANET. In Methods and Models in Computer Science (ICM2CS), 2010 International Conference on (pp. 112-116). IEEE.

[14]. Tseng, Y. C., & Hsieh, T. Y. (2002, October). Fully power-aware and location-aware protocols for wireless multi-hop ad hoc networks. In Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference on (pp. 608-613). IEEE.

[15]. Geetha, A, and Sreenath, N, Byzantine Attacks and its Security Measures in Mobile Adhoc Networks, Int'l Journal of Computing, Communications & Instrumentation Engg. (IJCCIE) Vol. 3, Issue 1 (2016) ISSN 2349-1469 EISSN 2349-1477.

[16]. Charles, D., Jain, K., & Lauter, K. (2006, March). Signatures for network coding. In Information Sciences and Systems, 2006 40th Annual Conference on (pp. 857-863). IEEE.

[17]. Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem" (PDF). ACM Transactions on Programming Languages and Systems. 4 (3): 382–401.

[18]. Perlman, R., Network Layer Protocols with Byzantine Robustness, MIT Thesis, August 1988.

[19]. Awerbuch, B., Holmer, D., & Rubens, H. (2003). Provably secure competitive routing against proactive Byzantine adversaries via reinforcement learning. John Hopkins University, Tech. Rep.

[20]. Awerbuch, B., Curtmola, R., Holmer, D., Nita-Rotaru, C. and H. Rubens, Mitigating Byzantine Attacks in AdHoc Wireless Networks, SecureCom'05, September 2005.

[21]. Vempaty, A., Ozdemir, O., Agrawal, K., Chen, H., & Varshney, P. K. (2013). Localization in wireless sensor networks: Byzantines and

mitigation techniques. IEEE Transactions on Signal Processing, 61(6), 1495-1508.

[22]. Kailkhura, B., Brahma, S., Han, Y. S., & Varshney, P. K. (2013, May). Optimal distributed detection in the presence of Byzantines. In ICASSP (pp. 2925-2929).

[23]. Han, K., Ravindran, B., & Jensen, E. D. (2007, September). Byzantine-tolerant, information propagation in untrustworthy and unreliable networks. In International Conference on Network-Based Information Systems (pp. 207-216). Springer, Berlin, Heidelberg.

[24]. Baras, J. S., Radosavac, S., Theodorakopoulos, G., Sterne, D., Budulas, P., & Gopaul, R. (2007, October). Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR. In Military Communications Conference, 2007. MILCOM 2007. IEEE (pp. 1-7). IEEE.

[25]. Jafarisiavoshani, M., Fragouli, C., & Diggavi, S. (2007, July). Subspace properties of randomized network coding. In Information Theory for Wireless Networks, 2007 IEEE Information Theory Workshop on (pp. 1-5). IEEE.

[26]. El-Hajj, W., Safa, H., & Guizani, M. (2011). Survey of security issues in cognitive radio networks. J. Internet Tech., 12(2), 181-198.

[27]. He, X., Dai, H., & Ning, P. (2013). A byzantine attack defender in cognitive radio networks: The conditional frequency check. IEEE Transactions on Wireless Communications, 12(5), 2512-2523.

[28]. Nie, G., Ding, G., Zhang, L., & Wu, Q. (2017). Byzantine Defense in Collaborative Spectrum Sensing via Bayesian Learning. IEEE Access.

[29]. Castro, M., Druschel, P., Ganesh, A., Rowstron, A., & Wallach, D. S. (2002). Secure routing for structured peer-to-peer overlay networks. ACM SIGOPS Operating Systems Review, 36(SI), 299-314.

[30]. Awerbuch, B., Holmer, D., Nita-Rotaru, C., & Rubens, H. (2002, September). An on-demand secure routing protocol resilient to byzantine failures. In Proceedings of the 1st ACM workshop on Wireless security (pp. 21-30). ACM.

[31]. Avramopoulos, I., Kobayashi, H., Wang, R. and A. Krishnamurthy, Highly Secure and Efficient Routing, INFOCOM'04, March 2004.

[32]. Awerbuch, B., Cole, R. G., Curtmola, R., Holmer, D., & Rubens, H. (2006). Dynamics of learning algorithms for the on-demand secure byzantine routing protocol. Lecture notes in computer science, 4357, 98.

[33]. Curtmola, R., & Nita-Rotaru, C. (2009). BSMR: byzantine-resilient secure multicast routing in multihop wireless networks. Mobile Computing, IEEE Transactions on, 8(4), 445-459.

[34]. Chen, R., Park, J. M., & Bian, K. (2008, April). Robust distributed spectrum sensing in cognitive radio networks. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE (pp. 1876-1884). IEEE.

[35]. Marano, S., Matta, V., & Tong, L. (2009). Distributed detection in the presence of Byzantine attacks. IEEE Transactions on Signal Processing, 57(1), 16-29.

[36]. Rawat, A. S., Anand, P., Chen, H., & Varshney, P. K. (2011). Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks. IEEE Transactions on Signal Processing, 59(2), 774-786.

[37]. Li, Z., & Oechtering, T. J. (2014, May). Tandem distributed Bayesian detection with privacy constraints. In Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on (pp. 8168-8172). IEEE.

[38]. Kailkhura, B., Han, Y. S., Brahma, S., & Varshney, P. K. (2015). Distributed Bayesian detection in the presence of Byzantine data. IEEE transactions on signal processing, 63(19), 5250-5263.

[39]. Hashlamoun, W., Brahma, S., & Varshney, P. K. (2017). Mitigation of Byzantine Attacks on Distributed Detection Systems using Audit Bits. IEEE Transactions on Signal and Information Processing over Networks.

Cite this article as :

S. Maharaja, R. Jeyalakshmi, A.V. Sabarish Kanna, M. Deva Priya, "Secured Routing in Mobile Ad hoc Networks (MANETs) ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 277-289, March-April 2019. Available at doi : https://doi.org/10.32628/CSEIT195275
Journal URL : http://ijsrcseit.com/CSEIT195275