International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 25, No. 2, April, 2020, pp. 173-181
Journal homepage: http://iieta.org/journals/isi

Preventing Malicious Packet Drops in MANETs by Counter Based Authenticated Acknowledgement

Mohammed Ali Hussain[1], Balaganesh Duraisamy[2*]

[1] Dept. of CSE, Lincoln University College, Petaling Jaya 47301, Malaysia
[2] Faculty of Computer Science & Multimedia, Lincoln University College, Petaling Jaya 47301, Malaysia

Corresponding Author Email: balaganesh@lincoln.edu.my

https://doi.org/10.18280/isi.250204

Received: 6 December 2019
Accepted: 25 February 2020

Keywords:
MANET, acknowledgment, packet drop, resource, mitigation and key agreement

ABSTRACT

Mobile ad hoc networks are a wireless infrastructure-free network composed of heterogeneous mobile nodes. A reliable mechanism can prevent malicious packet dropping nodes is end to end acknowledgment. However, packets drop from the intermediate node due to the insufficient resources such as buffer overflow and lack of energy, and there is a chance that the reputed intermediate nodes to become malicious due to their constrained resources. Furthermore, packets drop in the network is a noteworthy problem, and it negatively impacts network performance. Thus the existing acknowledgment mechanism must be incorporated with the mitigation mechanism of the packets drop due to constrained resources. Moreover, the security strength of the mechanism is further improved by providing integrity to the acknowledgment message and authentication to the acknowledgment sender. The goal of the paper is to enhance the existing acknowledgment based approach by providing authenticity to ACK packets and preventing packets drop due to constrained resources. Packet drops due to constrained resources are mitigated by selecting no-congested and energy-efficient intermediate nodes for communication. Authentication of ACK packets is achieved digested acknowledgment with the session key. Computation of session key is achieved by the Password-based authenticated key agreement based on the discrete logarithmic problem of Chebyshev polynomial based chaotic Maps. Performance results indicate that the computation complexity of the proposed key agreement protocol is less in comparison with modular exponential and elliptic curve-based key agreement protocols. The proposed method not only prevents the malicious packet dropping nodes but also prevents packet dropping due to constrained resources.

1. INTRODUCTION

A MANET (Mobile Ad-hoc Network) is a peer to peer infrastructure-free network comprises of heterogeneous and autonomous mobile nodes. The communication between mobile nodes happens through a medium of radio communication in a multi-hop manner. The characteristics of MANET include autonomous, self-maintenance, and self-configuration, make the network most suitable for deploying in a hostile environment. MANET environment is more defenseless towards the security threats compared to wired and wireless infrastructure-based networks. Furthermore, peer-peer networking capability that is nodes needs to perform the task of routing along with hosting, make the MANET venerable towards the security solutions. The network does not consist of any clear predefined place to organize security solutions [1].

The development aim of the MANETs is to enable network access everywhere all the time. The network is formed by the basis of infrastructure-less, self-maintained, and self-configured. Nodes present in the network are provided with the intelligence of the network; thus, they form a peer to peer network in the standalone fashion. The mobility of the nodes makes the topology of network dynamic and unpredictable. These characteristics make MANETs to cost and time effective and also lead it to deploy in sensitive and critical places. Communication between two nodes occurs straight if they present in the radio range of one another. Or else, the communication is enabled by relaying on the intermediate nodes. Thus, the nodes in a network need to act as a router to allow communication by forwarding the packets of other nodes [2].

A routing protocol is required to establish a path between communicating entities, to facilitate data communication within the network. The network protocol establishes the routes in a MANETs by the consideration that the nodes in a network are trustworthy and follow the networking protocols specifications. The consideration of the routing protocol is not valid in a hostile environment, such as in MANETs. The malicious actions in the MNAETs routing layer are possible by refusing the packets to forward or simply dropping the packets by the relaying nodes. Prime malicious activities are black hole attack, cooperative black hole attack, partial dropping, and false reporting. Packets dropping from relaying nodes in MANET is a noteworthy issue that negatively affects the performance of the network and particularly degrades the efficiency of a network [3].

In recent years, various security mechanisms designed to minimize the malicious packet dropping nodes from the network layer. The existing mechanisms primly divided as a credit-based mechanism, reputation-based mechanism, and acknowledgment based mechanism. Acknowledgment-based approaches are more auspicious than the credit and reputation-based mechanisms [4, 5].

The acknowledgment based mechanism aims to mitigate false reporting nodes along with packet dropping nodes by creating ACK (Acknowledgement) packets. Intermediate or destination node transmits the ACK packets to source about the successful reception packets. It does not consider the packets drop due to either insufficient buffer or due to insufficient energy. Thus it considered constrained packet dropping nodes to be malicious. Further, the reliability of the ACK approach depends on the integrity and authentication of the ACK packet.

Thus the ACK approach can be further improved by the mitigation mechanism of the packets drop due to constrained resources and integrity of the ACK packet. Improving mechanisms must be less overhead, as monitoring and detecting nodes present in a constrained network resource environment, i.e., nodes contain limited energy and buffer. Further, it is not possible to replace and recharge the node's battery during the communication operation. There is a requirement of energy conservation so that the nodes do not die due to exhaust of energy. Thus, the security algorithms in MANET must consider the constrained resource issue of the nodes so that they can be beneficial to be deployed on the battlefield. Thus the goal of providing integrity and authentication in the ACK approach is achieved by the method of authenticated key agreement among the communicating parties and digested acknowledgment with less computational overhead.

The goal of the paper is to enhance the acknowledgment based approach by mitigating packet drop due to constrained resources and authenticating ACK packets. Packet drops due to constrained resources are mitigated by selecting no-congested and energy-efficient intermediate nodes for communication. ACK packets authentication is achieved by digested acknowledgment with the session key. Computation of session key is achieved by the Password-based authenticated key agreement based on the discrete logarithmic problem of Chebyshev polynomial based chaotic Maps.

In comparison to the existing method, proposed work solves the issue of packet dropping due to constrained resources. The issue is solved by considering the packet drop due to buffer overflow and packet drop due to a lack of energy at the intermediate node. Further, it also reduces the overhead of authenticated key agreement, as MANET is infrastructure less, and its key agreement mechanism must not high overhead. Finally, improves the performance of the network by mitigating both malicious and unintentional packet dropping nodes from communication.

The remaining paper is organized as section 2 describes the related work, proposed work explains in section 3, performance analysis is described in section 4, and work ends with a conclusion followed by references.

2. RELATED WORK

MANETs is a wireless infrastructure-free, peer-peer networks. The characteristics of the network are mobility, dynamical networking topology, heterogeneity, peer-peer communication, self-forming, and adaptation. Characteristics of MANETs make it deploy in different types of critical and sensitive applications in different regions. These regions are health-care, vehicular communications, military and disaster relief. Thus the communication environment of MANETs should be secured.

Enabling communication in any network is achieved by the creation of the path between source and destination by routing protocols. Most routing protocols establish a route in MNAETs based on the assumption that the nodes in the network are trustworthy. The consideration of routing protocols is not faithful, as nodes perform the malicious actions by not following the protocol's specifications. The malicious activities are not forwarding the packets or simply dropping the packet from the routing layer. Such malicious activities are termed as selfish and malicious. Moreover, packets also get dropped due to constrained resources and broken links.

The nodes which drop the packets due to selfish and malicious behavior are known as misbehaving nodes and named as black hole, cooperative black hole, false reporting, and partial dropping attacks. The nodes which drop the packets due to overload and broken links are known as packets dropping due to constrained resources. Packets drop from the communication path is the noteworthy issue that negatively impacts the performance of the network and particularly degrades the efficiency of the network. It affects the packet delivery, and creates the congestion and disturbs the network resources. In particular, the issue of mitigation of the malicious packet dropping nodes along with packets drop due to constrained resources have been extensively deserted in current routing protocols developed for MANETs.

Existing work on misbehaving node mitigation is majorly divided into three parts, such as credit, reputation, and acknowledgment based mechanisms. The simple idea of a credit-based mechanism is to offer intensive to nodes for their consistent packet operation. Node gets credit for its reliable packet operations. Virtual-currency or appropriate payment system provides the credits. Nodes are either buyers or sellers of the packet operations. Nodes need to have enough credits to participate in communication [4].

Hubaux et al. [6] proposed a credit-based mechanism. In this mechanism of misbehaving nodes mitigation, each node needs to maintain a counter called "Nuglet Counter," with the predefined initial value. Counter value gets decreased when nodes send the packets of their own. The counter value is computed based on the estimated number of intermediate nodes that are needed to reach the destination. The counter value gets incremented when the nodes forward the packets of other nodes. The system put the condition that counter must be positive about participating in communication so that nodes are fortified to remain the helping other nodes. Tamper resistance hardware monitors and regulates the illegal incrimination of the nuglet counter.

Sakuna et al. [7] proposed another credit-based Approach. The nodes in the network give the credits to their neighboring nodes. Credits are initiated in a route-finding as well as data forwarding phases. The computation of credits is as follows, by Eqns. (1) and (2).

$$Cr_i = 3 * (H_c) \tag{1}$$

$$Cr_{max} = 5 * (H_c + 2) \tag{2}$$

where, Cr_i is initial credit, Cr_{max} is maximum credit, and H_c is hop count. Credits decrease when the node cannot receive the acknowledgment. Misbehaving nodes are decided on the criteria as the node will be untrusted when credit reaches zero.

The credit-based system is not scalable due to the centralized payment mechanism. Each node needs to maintain the extra hardware for tamper-proofing that may cause the overhead for the system. Moreover, the system needs to protect the payment mechanism. Reputed nodes might be punished indirectly due to their location, as they could not participate in communication to gain the credits. A node can maliciously sell the same packet several times to earn the number of credits. Thus this system is not much suitable for deploying in a constrained distributed environment such as MANET.

Another approach to mitigate the malicious packets dropping nodes from the communication path in MANETs is the reputation-based mechanism. The basic idea of reputation-based mechanism is to calculate reputation information of nodes by monitoring processes either directly or indirectly. In the direct investigation, every node directly monitors its neighbor node and recognizes the behavior. The indirect investigation, where a node may receive the reputation evidence from deciding the node's neighbor. Node gives higher priority to direct investigation. But Indirect Investigation is used to strengthen the direct investigation. The mechanism works on the foundation of gathering, upholding, and distributing reputation evidence of the nodes. Nodes with a higher reputation get services, and nodes with less reputation are isolated [4].

Thachil and Shet proposed a reputation-based mechanism [8]. In this approach, each node keeps track of the reputation value of the neighbor node by promiscuous monitoring. Reputation cost is computed as the ratio of the number of packets dropped with forwarded packets, in the range of '0 to 1'. If reputation value is reached below the predefined threshold cost, then the node treated as a misbehaving node. Identified malicious node informed to other nodes existing in the network through broadcasting.

Durgesh and Patil. Proposed another **r**eputation based Approach [9]. This approach initially finds the neighboring node of the RREP originator and named as the suspected node. Instructs that suspected node to listen to all the packets sent by the suspicious node. The mechanism maintains two counters named as Fcount and Rcount. Whenever the neighbor node forwards the packets to the suspected node, then the Fcount value is incremented. Rcount is incremented when the suspected node further forwards the received packet. Thus, this work aims to develop an effective routing protocol to minimize the packet dropping attacks from the routing path in MANET. Malicious node is detected when Fcount higher than the predefined threshold value.

The reputation-based approach is more promising than the credit-based approach, as there is no requirement of a central payment or credit system. Moreover, it does not require any extra hardware on each node. The system increases network scalability by designing the system in a distributed way. The mechanism entirely depends on the monitoring component of the node. The system does not work efficiently in the existence of packet drops due to constrained resources.

Another way of misbehaving mitigation mechanism is an acknowledgment based mechanism. The acknowledgment based mechanism aims to mitigate false reporting nodes along with packet dropping nodes. Intermediate or destination node sends the ACK packet to source about the successful reception packets. The different techniques of ACK approaches are n–hop Acknowledgement, where n=1,2,3.., end to end acknowledgment, and selective acknowledgment [4].

Two ACK [10], it detects the packet dropping nodes by acknowledging each data packet. The node that is two-hop away from the data packet sending node needs to replay with the ACK packets. If two ACK packet did not receive in an appropriate duration of time, then the intermediate nodes conveyed as misbehaving. This approach solves the false issue report, which could not be solved by credit and reputation-based approaches. However, the system contains the overhead of transmitting the ACK packet for every data packet.

AACK (Adaptive Acknowledgement) [11], it is a combination of two approaches, i.e., TACK (Two Acknowledgement) and end to end ACK. When the destination node receives the packets, then it transmits ACK packets to the source along with the opposite order of the similar route. If the source did not receive the ACK within an appropriate time interval, then it switches to TWO-ACK. ACK mechanism is more favorable than the reputation-based mechanism, due to fewer overhead of computation and memory utilization. The approach majorly depends on the reputation of the ACK packet. Hence ACK packets must be valid and authentic. It must also consider the mitigation of packet dropping due to constringed resources to enhance network performance.

In particular, the issue of mitigation of the malicious packet dropping nodes along with packets drop due to constrained properties has been extensively deserted in current routing protocols designed for MANET. Different mechanisms presented in the literature to prevent the malicious packet dropping by an intermediate node. One of the reliable mechanisms to prevent malicious packet dropping is the end to end acknowledgment. However, packets can also drop from the intermediate nodes due to the constrained properties such as buffer overflow and lack of energy. Then there is a chance that the reputed nodes to become malicious due to their constrained resources. Furthermore, packets drop in the network is a noteworthy problem, and it negatively impacts network performance. Thus the existing acknowledgment packet dropping mitigation mechanism must be incorporated with the mitigation mechanism of the packets drop due to constrained resources. Moreover, the security strength of the proposed mechanism is further improved by the integrity of acknowledgment packets and authentication of the ACK packet sender.

Thus the goal of the paper is to enhance the acknowledgment based approach by authenticating ACK packets, and mitigating packets drop due to constrained resources. Packet drops due to constrained resources are mitigated by selecting non-congested and energy-efficient intermediate nodes for communication. Authentication of ACK packets is achieved digested acknowledgment with the session key. The session key is established by Password-based authenticated key agreement based on the discrete logarithmic problem of Chebyshev polynomial based chaotic Maps.

3. PROPOSED WORK

The proposed work is an extension of the acknowledgment based approach with the following considerations:

1. Selection of non-congested and energy-efficient intermediate nodes for communication
2. Session key agreement using Password-based authenticated key agreement based on the discrete

logarithmic problem of Chebyshev polynomial based chaotic Maps

3. Counter based end to end acknowledgment
4. Authentication of ACK packets by message digest and session key

System model

In this paper, we consider Multi-hop Mobile Ad hoc Networks with the number of nodes distributed in the radio communication area with heterogeneous recourses. The network is composed of reputed nodes, malicious nodes, and constrained nodes. Reputed nodes follow the routing protocol specification and do not drop the packets. Malicious nodes drop the packets and do not follow the by not following routing protocol specification. Constrained nodes drop the packets due to insufficient buffer and lack of energy. An Intermediate node of the routing path needs to forward the packets from multiple sources. Packets have arrived from a large number of independent sources towards the intermediate node. Therefore, MANET needs a routing protocol to mitigate the packet dropping from the communication path.

In our scheme, we designed counter-based authenticated acknowledgment to mitigate both packets drop due to constrained nodes and malicious nodes. The considering non-congested energy-efficient nodes mitigate constrained nodes for communication path. Malicious packet drops mitigated by counter-based digested acknowledgment.

3.1 Selection of non-congested and energy-efficient intermediate nodes for communication

The aim of selecting non-congested and energy-efficient nodes for communication is to prevent the packets drop due to constrained resources as well as to prevent the reputed nodes from becoming malicious. The objective is achieved by the selection of the nodes for the routing path, which contains the sufficient buffer size as well as sufficient energy, and it is achieved as follows:

The average number of packets are queued at the buffer of the node is computed by the help of RED gateway the following Eq. (3).

$$\begin{aligned}\text{Averagenewqueue}(Q_{avrg}) &= (\text{Weighted constant}) \\ &\quad * \text{Instant Queue} \\ &\quad + (1 - \text{Weighted constant}) \\ &\quad * \text{Averageoldqueue}\end{aligned} \tag{3}$$

The computed queue size must be less than the certain level of handling capacity of the node, i.e., threshold value, so that it could not drop the packets due to buffer overflow. The threshold value is computed by the following Eq. (4)

$$(Q_{Th}) = 75\%\ of\ buffer\ size \tag{4}$$

where, Q_{Th} is considered as theshold buffer size, which is indicating that 75 % of buffer is full.

Packet handling ability of node due to residual energy of the node is computed by the following Eq. (5)

$$\begin{aligned}\text{Energy} - \text{Packet handling ability } (Ep) \\ = \frac{\boldsymbol{E - E(P_i)}}{\boldsymbol{E_t + E_r + E_p}} \\ \forall\ \boldsymbol{E - E(P_i) \geq\ E_r + E_p + E_t \ldots}\end{aligned} \tag{5}$$

where, E is the energy of node, $E(\boldsymbol{P_i})$ is energy consumed by node to process the packet $\boldsymbol{P_i}$. $\boldsymbol{E_r, E_p}$ and $\boldsymbol{E_t}$ are energy consumed for receiving, processing and transmitting, the packet respectively.

The computed energy efficiency value must be higher than the certain level of handling capacity of the node, i.e., threshold value, so that it could not drop the packets due to lack of energy. The threshold value is computed by the following Eq. (6)

$$Ee_{Th} = \frac{(75\%) * E}{\boldsymbol{E_r + E_t + E_p}} \tag{6}$$

During the routing process, the nodes which satisfy the threshold condition of buffer and energy by equations (4) and (6) are only considered for intermediate nodes. Thus the packets drop due to constrained resources is minimized. The logical procedure of the constrained node detection prevention is shown in Table 1.

Table 1. Non-congested and energy efficient node detection

```
Algorithm 1: Function Non-congested and energy efficient node detection
Input: $Q_{Th}, Ee_{Th}$
Output: Constrained nodes
Session[i] mapped to Non-congested and energy efficient node detection
If calculation interval= true then
    For session[i]
        Calculate
        $Ep$ && $Q_{avrg}$
    End for
Else wait for calculation interval
While tuning interval= true
    If $Ep \leq Ee_{Th}$ && $Q_{avrg} \geq\ Q_{th}$
        Session[i]= constrained nodes
    Else
        Consider the node in route computation
    End if
End if
Wait for tuning interval
End if
```

3.2 Session key agreement using Password-based authenticated key agreement based on the discrete logarithmic problem of Chebyshev polynomial based chaotic Maps

Authentication and session key agreement aims to provide the integrity to ACK packets of acknowledgment approach and also provide the authentication of the ACK packet sender. The MANETs need the authenticated key agreement mechanism with the least computational overhead due to its characteristics.

The obligation is fulfilling by the development of the mechanism based on the discrete logarithmic property of Chebyshev polynomial, where the computational overhead is free from scalar multiplication and modular exponent. Moreover, the proposed key is computed with the help of the "Discrete Logarithmic problem" property of Chebyshev polynomial based Chaotic Maps [12], which might not be conceivable to compute in polynomial time by an attacker.

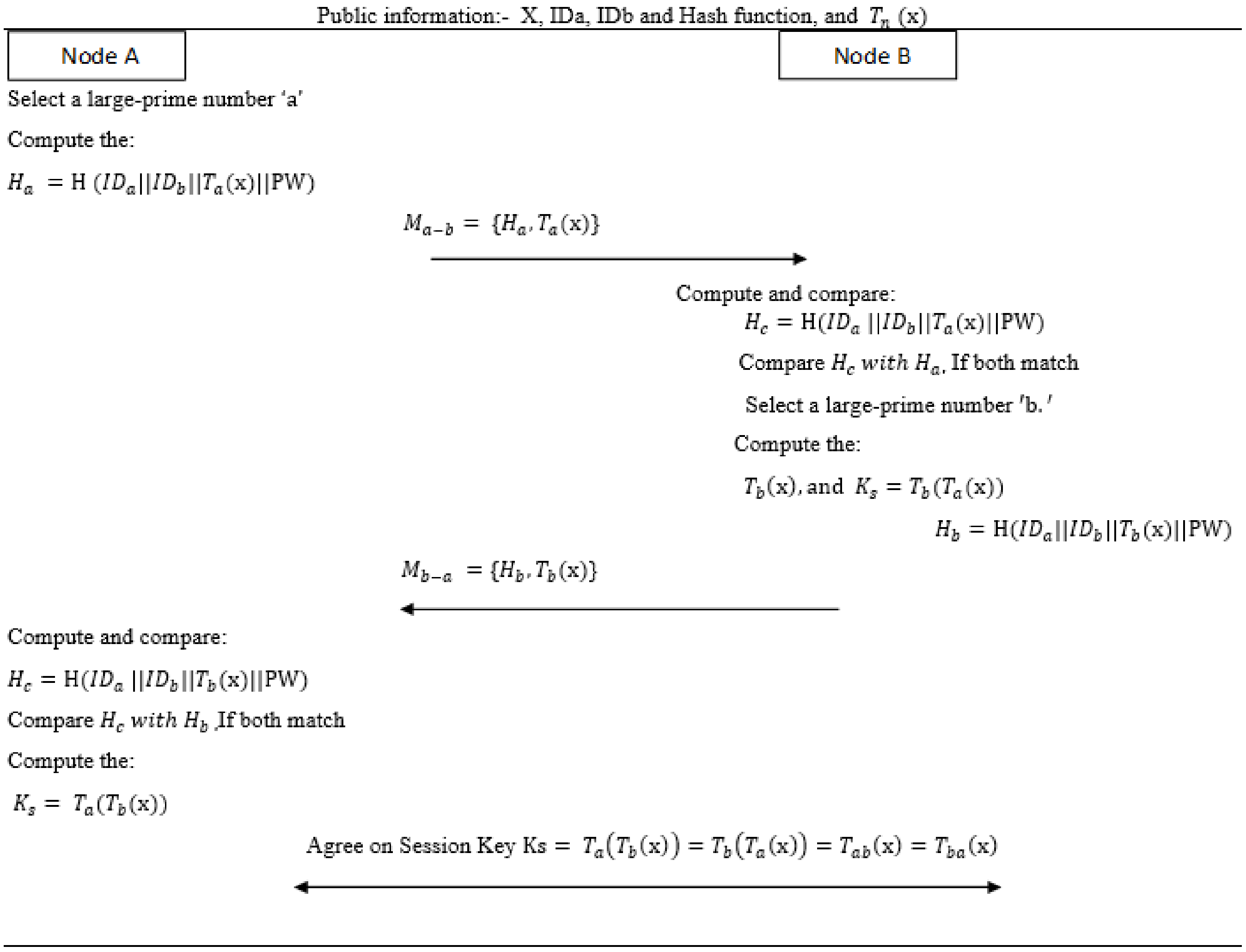
Public information:- X, IDa, IDb and Hash function, and T_n (x)
Node A
Node B
Select a large-prime number 'a'
Compute the:
H_a = H ($ID_a||ID_b||T_a$(x)||PW)
$M_{a-b} = \{H_a, T_a(x)\}$
Compute and compare:
H_c = H(ID_a $||ID_b||T_a$(x)||PW)
Compare H_c with H_a. If both match
Select a large-prime number 'b.'
Compute the:
T_b(x), and $K_s = T_b(T_a(x))$
H_b = H($ID_a||ID_b||T_b$(x)||PW)
$M_{b-a} = \{H_b, T_b(x)\}$
Compute and compare:
H_c = H(ID_a $||ID_b||T_b$(x)||PW)
Compare H_c with H_b .If both match
Compute the:
$K_s = T_a(T_b(x))$
Agree on Session Key Ks = $T_a(T_b(x)) = T_b(T_a(x)) = T_{ab}(x) = T_{ba}(x)$

Figure 1. The authentication and session key agreement between A and B

In MANETs, the authentication process must be performed between communicating parties before they exchange the information. Further, it is difficult to perform the authentication between all the nodes present in the network due to its characteristics. To attain authentication between communication parties, end to end authenticated, key agreement protocol is proposed. Finally, the paper designs end to end authenticated key agreement mechanism with less computational cost. The proposed key agreement provides the mutual authentication, session key agreement, and prevents security threats such as man in the middle, guessing attacks.

In literature, Shin et al. [13], designed hybrid crypto-based two-party authentication in MANETs with the help of RSA. Zhu et al. [14] verified that RSA based authentications are effective and secure against different security threats. Further, Tan et al. [15] analyzed RSA based authentications and determined that large communicational overhead is needed to verify the RSA public key. Thus we design a Password-based end to end the authenticated key agreement for MANET with the help of chaotic Maps. The algorithm explanation is as follows:

The nodes present in the network contains a unique identity (ID_i), $(i = 1, 2, \dots)$. The nodes get the password through a secure channel. During the registration, each node gets the parameters such as integer value $'X'$ and hash function H(.) Then, the nodes compute the public information by selecting the large private prime value $'k'$ by using the following Eq. (7).

$$\mathrm{T_k(x)} = 2\,\mathrm{x} * \mathrm{T_{k-1}(x)} - \mathrm{T_{k-2}(x)} * (\mathrm{mod\ N}), \quad \mathrm{k} \geq 2 \qquad (7)$$

Consider the end to end authentication between two nodes, i.e., source node as A and destination node as B with public information $\{(ID_a, T_{k_a}(x))\}$ and $\{(ID_b, T_{k_b}(x))\}$ and private information k_a, and k_b respectively. The authentication and session key agreement between A and B is explained in Figure 1.

In Figure 1, X is the integer value, IDa, and IDb are the identities of node A and node B respectively. H(.) Is the hash function and T_n (x) is the chaotic Maps based chebeshive polinomial function, as shown in Eq. (7).

3.4 Counter based end to end digested acknowledgment

The paper designs the counter-based ACK approach to preventing malicious packets from dropping nodes. Instead of sending the ACK packets for each data packet or two data packets, it sends the ACK packet after the predefined time interval. Initially, source and destination agree on the time interval for generating, sending, and receiving the ACK packets. During communication, the source transmits the data packets to the destination and count the number of packets transmitted within a predefined time interval, say T_s, and gets the successful reception of packets at the destination after the time interval say, T_{ack}. The time interval of the T_{ack} is decided by the following Eq. (8).

$$T_{ack} = T_s + RTT + T_{add} \tag{8}$$

where,

$RTT = Round\ trip\ time$

T_{add} = The time required to construct the ACK, which includes message digest computation time

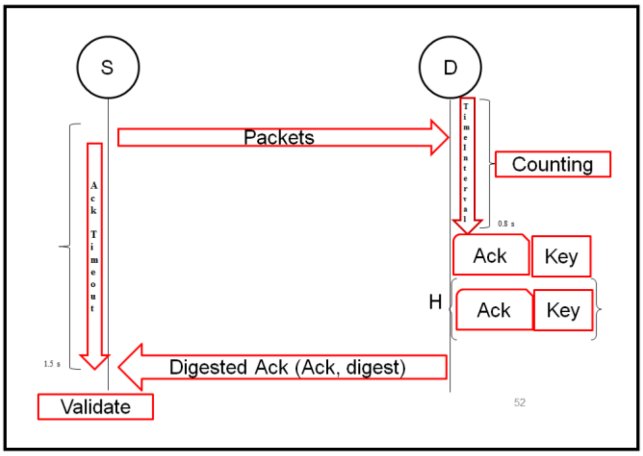

Figure 2. Counter based digested ACK between source to destination

The destination constructs the ACK packet and transmits it to the source. Instead of constructing ACK for all the received packets, the destination only constructs the ACK packets for the number of packets received within a time interval T_s.

Initially, all the nodes agree to the time intervals to count the sending packets and creating the Acknowledgement packet. During communication, sender and destination node tracks and counts the sent and received packets within the predefined time interval T_s . Then destination constructs the acknowledgment packet with the entries of the number of packets received and agreed on an interval of time. Now, the destination adds the session key agreement by the authenticated key agreement using chaotic maps by Figure 1. Then, the destination creates a message digest and appends the digested message along with the acknowledgment packet as follows:

If both match, the source considers that the information is not altered during communication. If the source does not receive the ACK packet or ACK packet is not validated by the source, then the source confirms that there is an intentional misbehaving node present in a routing path. The counter-based digested acknowledgment mechanism is shown in Figure 2, and algorithm steps are shown in Table 2. The combination of both counter-based acknowledgment and selection of energy-efficient non-congested neighbors prevent the packet drops due to malicious packet dropping as well as packet dropping due to constrained resources.

The proposed method overcomes the problem of sending either the ACK packet for every data packet sent, instead it only SNED the ACK packet during the predefined time interval. Thus the method greatly reduces the overhead of the network. The method also validates the ACK packet by authenticated key to prevent the false report form a malicious intermediate node.

Table 2. Malicious packet drop node detection

```
Algorithm 2: Function Malicious packet dropping nodes detection
Input: Ack,$T_{ack}$
Output: Malicious packet dropping nodes
Session[i] mapped to Malicious packet drop node detection
For session[i]
do
1. Source sends the packet to a destination up to time interval $T_s$ and wait until $T_{ack}$
2. Destination starts the counter to sum the number of packets received during the agreed time-interval.
3.The destination node creates an ACK packet and includes the number of packets received in the ACK packet and append the agreed session key, and then the node creates the digest of created ACK packet with the MD5 algorithm as follows:
    m=Acknowledgement packet X or Session Key of destination
                digested message (d)=H(m)
4. The destination sends the original acknowledgment packets along with the digested message to the source node with a similar route in reverse direction.

If (source did not receive the ACK packet || ACK packet is not authenticated)

An intermediate node in the route is malicious packet dropping node
Else
Nodes are reputed and continue the communication.
```

4. PERFORMANCE ANALYSIS

NS-2 simulator is used to evaluate the performance of the proposed protocol. The parameters considered for the performance analysis are shown in Table 3. The simulation environment consists of the number of nodes that are mobile inside the network with a random waypoint mobility model with 25 m/s pause time. The initial energy of the node is set to 20 joules with a fixed radio communication range of 250m, and the node sends the information with a rate of 2 Mbps. The receiving and transmitting power of the node is set to 300mW and 600mW, respectively. The duration of the simulation is set to 1000s, and considered performance is an average of 3 performance scenarios. The node in the network is divided into three categories. The first category is reputed nodes, which follow the routing protocol specifications, the second category is the nodes that drop the packets due to constrained energy and buffer overflow, and the third category is malicious packet dropping nodes. Threshold values considered for simulation are as follows:

1. $T_{ack} = 0.15\ s$
2. $T_s = 0.8s.$
3. $Ee_{Th} = 625\ Kbytes$
4. $Q_{Th} = 312.5\ Kbytes$

Threshold values could be set at the time of network initialization. Depending on the sensitivity and application of the network, the threshold values could be changed.

Performance evaluation metrics considered for performance evaluations are throughput, packet delivery fraction, and control packet overhead and energy efficiency. The prime objective of the paper is to evaluate the performance of the proposed method (ERMMN) under the network, which consists of packet dropping nodes due to misbehaving activities as well as insufficient resources. Further, we compare the performance with the existing secure knowledge algorithm (SKA) [16] and acknowledgment based algorithm (AACK) [4] and reactive routing protocol with no packet dropping nodes (AODV-NM) [17]. The performance results are shown in Figures 3-10.

Table 3. Simulation parameters of MANET

Simulation- Parameters	Values
Duration	1200 s
Nodes	100 to 400
Link Layer	Logical Link
MAC	802.11
Communication	Two-Ray Ground
Mobility-model	Random-waypoint
Network layer	Reactive routing
Queuing-technique	Priority-queue
Energy	100 j
Traffic	CBR
Network area	1000m x1 000m

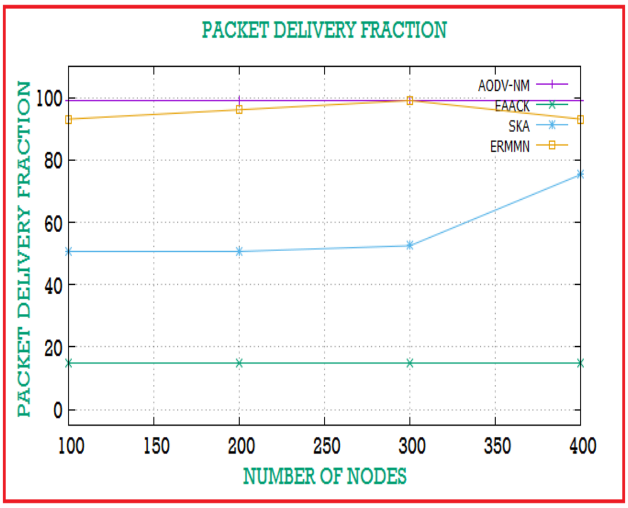

Figure 3. PDF comparison with respect to a varying number of nodes

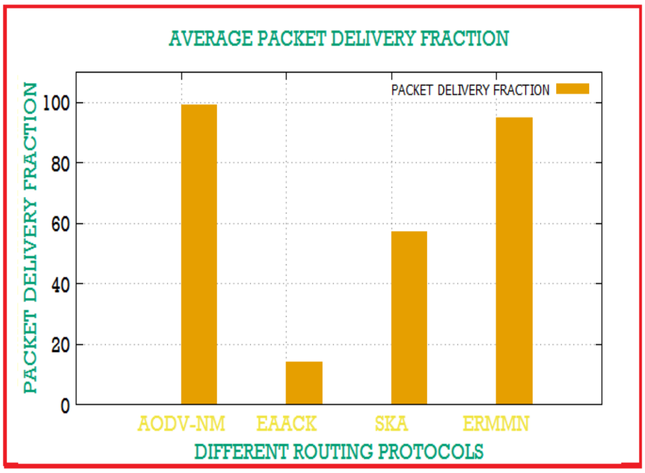

Figure 4. Average PDF of proposed and existing approaches

The packet delivery fraction proposed method is almost equal to the AODV-NM and better than SKA and EAACK. EAACK Performance is low as it does not consider the mitigation of packet drop due to constrained resources. The results of the PDF are shown in Figures 3 and 4.

The throughput of the network is computed with the variable number of nodes and simulation time in the presence of an intentional and unintentional misbehaving node. The proposed mechanism throughput is better than EAACK and SKA algorithms, as it prevents the packets from dropping due to constrained resources. The results of throughput are shown in Figures 5, 6, and 7.

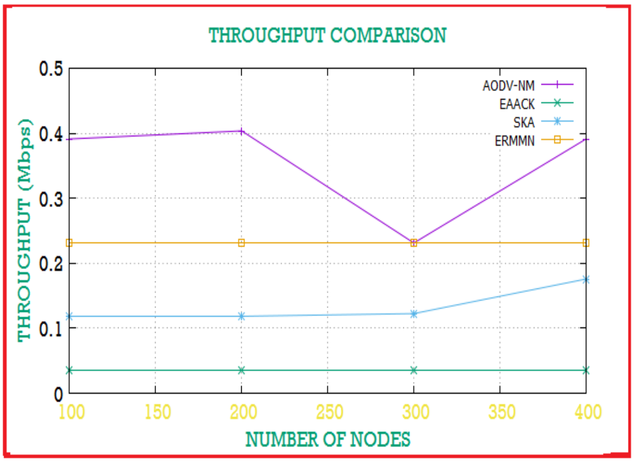

Figure 5. Throughput (Mbps) comparison with respect to a varying number of nodes proposed and existing approaches

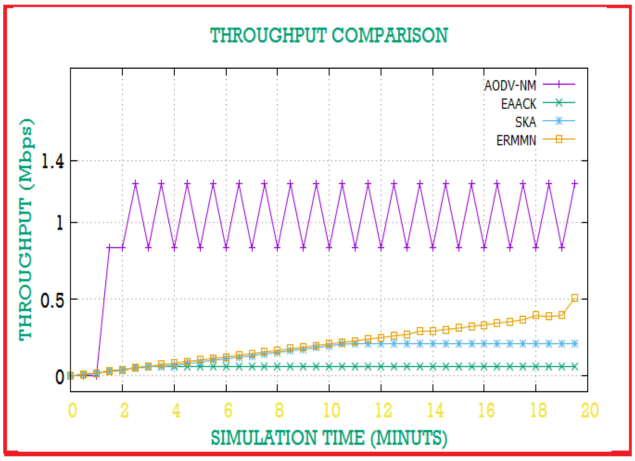

Figure 6. Throughput (Mbps) comparison with respect to the simulation time (minutes) proposed and existing approaches

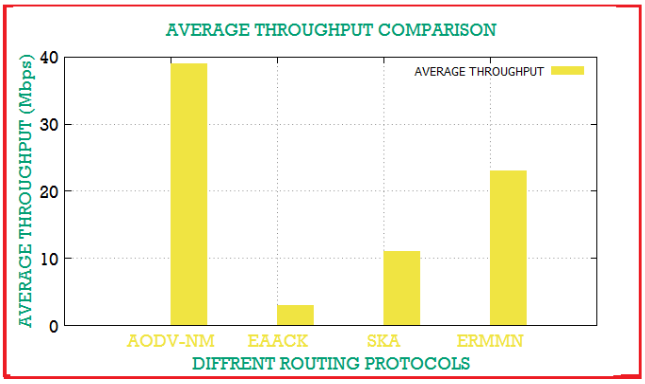

Figure 7. Average throughput (Mbps) comparison of proposed and existing approaches

The overhead of the network is computed in control packets with respect to the number of nodes. Figure 8 is clearly indicating that the EAACK overhead is high in comparison with other approaches. SKA protocol control packets overhead is less than EAACK and ERMMN, as it did not consist of acknowledgment packets.

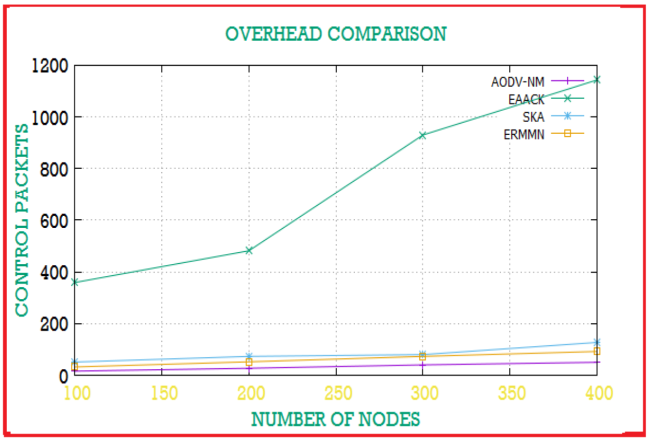

Figure 8. Routing packet overhead comparison with respect to a varying number of nodes proposed and existing approaches

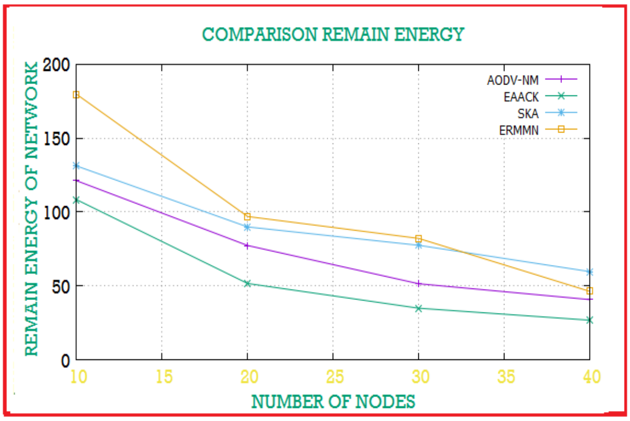

Figure 9. Average reaming energy of nodes in network comparison with respect to the varying number of nodes proposed and existing approaches

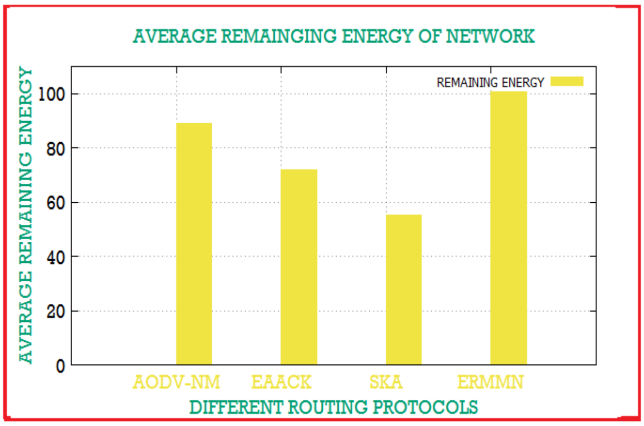

Figure 10. Average reaming energy of nodes in network comparison of proposed and existing approaches

Energy consumption of the network is computed with respect to the number of nodes and also compared with packet delivery fraction and throughput of the network.

Proposed method network remaining energy more as it considers the energy efficiency metric during the routing process. Existing protocols remaining energy is less as there is no consideration of energy efficiency during the routing process. The energy efficacy results are shown in Figures 9 and 10.

The results 3-10 are clearly indicating that the proposed work greatly improves the performance of the network in terms of packet delivery, delay, and energy efficiency. The paper, compute and analyses the performance results with respect to simulation time and the number of nodes, to demonstrate how the prosed work efficiently improve the performance in different scenarios.

5. CONCLUSION

One of the reliable mechanisms to prevent malicious packet dropping is the end to end acknowledgment. However, packets may also drop from the intermediate nodes due to the constrained resources such as buffer overflow and lack of energy. Then there is a chance that the reputed nodes to become malicious due to their constrained resources. Furthermore, packets drop in the network is a noteworthy problem, and it negatively impacts on the network performance. Thus the existing acknowledgment packet dropping mitigation mechanism must be incorporated with the mitigation mechanism of the packets drop due to constrained resources. Moreover, the strength of the mechanism is further improved by the integrity of the acknowledgment message and authentication of the acknowledgment sender. Thus the goal of the paper is to enhance the acknowledgment based approach with the mitigation of packet dropping due to constrained resources and authentication of ACK packets. Packet drops due to constrained resources are mitigated by selecting no-congested and energy-efficient intermediate nodes for communication. Authentication of ACK packets is achieved digested acknowledgment with the session key. A session key is computed by the Password-based authenticated key agreement based on the discrete logarithmic problem of Chebyshev polynomial based chaotic Maps. Performance results indicated that the computation complexity of the proposed key agreement protocol is less in comparison with modular exponential and elliptic curve-based key agreement protocols. Finally, the proposed mechanism prevents the malicious packet dropping nodes along with the packet dropping due to constrained resources.

REFERENCES

[1] Mohammad, A.A.K., Mahmood, A.M., Vemuru, S. (2019). Intentional and unintentional misbehaving node detection and prevention in the mobile ad hoc network. International Journal of Hybrid Intelligence, 1(2-3): 239-267. https://doi.org/10.1504/IJHI.2019.103580

[2] Hoebeke, J., Moerman, I., Dhoedt, B., Demeester, P. (2004). An overview of mobile ad hoc networks: applications and challenges. Journal-Communications Network, 3(3): 60-66.

[3] Shakshuki, E.M., Kang, N., Sheltami, T.R. (2013). EAACK—a secure intrusion-detection system for MANETs. IEEE Transactions on Industrial Electronics,

60(3): 1089-1098. https://doi.org/10.1109/TIE.2012.2196010

[4] Liu, K.J., Deng, J., Varshney, P.K., Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5): 536-550. https://doi.org/10.1109/TMC.2007.1036

[5] Abbas, S., Merabti, M., Llewellyn-Jones, D. (2010). A survey of reputation-based schemes for MANET. The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK.

[6] Buttyán, L., Hubaux, J.P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications, 8(5): 579-592. https://doi.org/10.1023/A:1025146013151

[7] Saetang, W., Charoenpanyasak, S. (2012). Caodv free blackhole attack in ad hoc networks. International Conference on Computer Networks and Communication Systems (CNCS, 2012), 35: 63-68.

[8] Thachil, F., Shet, K.C. (2012). A trust-based approach for AODV protocol to mitigate black hole attack in MANET. 2012 International Conference on Computing Sciences, Phagwara, India. https://doi.org/10.1109/ICCS.2012.7

[9] Kshirsagar, D., Patil, A. (2013). Blackhole attack detection and prevention by real-time monitoring. 2013 Fourth International Conference on Computing, Communications, and Networking Technologies (ICCCNT), Tiruchengode, India. https://doi.org/10.1109/ICCCNT.2013.6726597

[10] Ukey, A.S.A., Chawla, M. (2010). Detection of packet dropping attack using improved acknowledgment based scheme in MANET. IJCSI International Journal of Computer Science Issues, 7(4): 12-17.

[11] Al-Roubaiey, A., Sheltami, T., Mahmoud, A., Shakshuki, E., Mouftah, H. (2010). AACK: Adaptive acknowledgment intrusion detection for MANET with node detection enhancement. 2010 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, WA, Australia. https://doi.org/10.1109/AINA.2010.136

[12] Zhu, H.F. (2015). Flexible and password-authenticated key agreement scheme based on chaotic maps for multiple servers to server architecture. Wireless Personal Communications, 82(3): 1697-1718. https://doi.org/10.1007/s11277-015-2307-4

[13] Shin, S.H., Kobara, K., Imai, H. (2007). An efficient and leakage-resilient RSA-based authenticated key exchange protocol with a tight security reduction. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 90(2): 474-490. https://doi.org/10.1093/ietfec/e90-a.2.474

[14] Zhu, F., Wong, D.S., Chan, A.H., Ye, R. (2002). Password authenticated key exchange based on RSA for imbalanced wireless networks. International Conference on Information Security. Springer, Berlin, Heidelberg, pp. 150-161. https://doi.org/10.1007/3-540-45811-5_11

[15] Tan, S.C., Zhu, H., Wang, Y.M. (2009). Some notes on a password-authenticated key exchange based on RSA. 2009 International Conference on Computational Intelligence and Security, Beijing, China. https://doi.org/10.1109/CIS.2009.225

[16] Siddiqua, A., Sridevi, K., Mohammed, A.A.K. (2015). Preventing black hole attacks in MANETs using secure knowledge algorithm. 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India. https://doi.org/10.1109/SPACES.2015.7058298

[17] Sana, A.B., Iqbal, F., Mohammad, A.A.K. (2015). Quality of service routing for multipath Manets. 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India. https://doi.org/10.1109/SPACES.2015.7058300