IEIE Transactions on Smart Processing and Computing, vol. 4, no. 2, April 2015
http://dx.doi.org/10.5573/IEIESPC.2015.4.2.115

Trust Predicated Routing Framework with Optimized Cluster Head Selection using Cuckoo Search Algorithm for MANET

J Chandra Sekhar and R Sivarama Prasad

Department of Computer Science and Engineering, Acharya Nagarjuna University / Nagarjuna Nagar, Guntur, Andhra Pradesh, India jcsekhar9@gmail.com, raminenisivaram@yahoo.co.in

***** Corresponding Author: J Chandra Sekhar

Received November 20, 2014; Revised December 27, 2014; Accepted February 12, 2015; Published April 30, 2015

** Regular Paper*

***Abstract*:** This paper presents a Cuckoo search algorithm to secure adversaries misdirecting multi-hop routing in Mobile ad hoc networks (MANETs) using a robust Trust Predicated Routing Framework with an optimized cluster head selection. The clustering technique designed in this framework leads to efficient routing in MANETs. The heavy work load in the node causes an energy drop in cluster head, which leads to re-clustering of the group, and another cluster head is selected to avoid packet loss during data transmission. The problem in the re-clustering process is that the overall efficiency of the routing process is reduced and the processing time is increased. A Cuckoo search based optimization algorithm is proposed to solve the problem of re-clustering by selecting the secondary cluster head within the initially formed cluster group and eliminating the re-clustering process. The proposed framework enables a node to select a reliable and secure route for MANET and the performance can be evaluated by comparing the simulated results with the AODV routing protocol, which shows that the performance of the proposed routing protocol are improved significantly.

***Keywords*:** Mobile Ad-hoc networks, Routing, Trust-predicated routing, Cluster head optimization, Cuckoo search algorithm

1. Introduction

In recent years, Mobile ad hoc networks (MANETs) are recognized discretely because of their mobility feature, dynamic topology and facilitate of deployment. A mobile ad hoc network is a self-organized wireless network with mobile contrivances that move freely in a network, such as laptops, cell phones and PDAs (Personal Digital Assistants) [1]. MANETs combine wireless communication with high degree node mobility unless the conventional wired networks do not have a fine-tuned infrastructure (base stations, centralized management points, etc.) [2]. The amalgamation of nodes in MANET forms an arbitrary topology, which can provide an extremely flexible method of establishing communications in many situations [3].

Multi-hop wireless links are used for communication between each mobile node in ad hoc networks. Each node acts as a router and forwarding data packets for other nodes due to a lack of infrastructure in conventional networks. The development of dynamic routing protocols have focused most on precursor research in ad hoc networks that can efficiently perceive the routes between two communicating nodes [4, 5]. The congenital nature of wireless ad hoc networks makes them quite susceptible to attacks ranging from passive eavesdropping to active interference [6]. A routed communication path between two nodes cannot be made totally free of malevolent nodes that will, in some way, not comply with the employed protocol and endeavor to interfere with the network operation. Unlike wired networks, where supplemental bulwark mechanisms can be deployed facilely in routers and gateways, a malicious node can paralyze the entire wireless network by disseminating erroneous routing information [7].

Secure ad hoc network routing protocols are difficult to

design due to the highly dynamic nature of an ad hoc network and the need to operate efficiently with limited resources, including the network bandwidth and the CPU processing capacity, memory and battery power (energy) of each individual node in the network [8]. Existing insecure ad hoc network routing protocols are often highly optimized to spread new routing information as quickly as conditions change, requiring a more rapid and often more frequent routing protocol interactions between the nodes than is typical in a traditional (e.g., wired and stationary) network [9]. Expensive and cumbersome security mechanisms can delay or prevent such exchanges of routing information, leading to reduced routing effectiveness, which may consume excessive network or node resources, leading to many new opportunities for possible Denial-of-Service attacks through a routing protocol [10, 11].

A number of secured routing protocols have been proposed for ad-hoc networks to mitigate the effects of misbehaving routers on the network performance (see e.g., [12] for a survey). These protocols use a range of mechanisms, such as cryptographic coding, multi-path routing and anomaly detection techniques, to increase the resistance of the protocol against attacks. Unfortunately, the design of secure routing protocols is an error-prone activity, and most of the proposed secure ad-hoc network routing protocols are still vulnerable to attack [13]. This suggests that the design of secure ad-hoc network routing protocols should be based on a systematic approach that minimizes the number of mistakes made in the design.

This paper proposes a robust Trust Predicated Routing Framework for secure routing with an optimized cluster head selection using a Cuckoo search algorithm to secure the MANETs against adversaries misdirecting the multi-hop routing. The proposed TPR framework clusters the MANET to secure path routing. Owing to the heavy work load in the node cluster, the head runs out of energy at normal routing process. This leads to re-clustering in which the group utilizes conventional secure routing approaches that elects another cluster head to avoid packet loss during data transmission. Therefore, the problem of the conventional system is that the overall efficiency of the routing process is reduced and the processing time is increased. The group does not need to be re-clustered using the proposed Cuckoo search based optimization algorithm, which selects the secondary cluster head within the initially formed cluster group to overcome the problem. The idea of the proposed framework is to enable a node to keep track of selecting a reliable and secure route for MANETs.

2. Related Work

Most previous work focused mainly on the routing as well as the exploration of attacks on routing by intruders. As it is agreed that routing and security process are no different, the track is such that the routing process is seen from a security perspective. V.Balakrishnan et al. [14] proposed an obligation predicated model fellowship to alleviate these attacks, such as flooding and packet drop attacks in MANETs. The system defined the rate inhibition, enforcement and recuperation for framing the model parameters of the fellowship. The fellowship together with the trust or security protocols can be used for further enhancement of the efficiency and ameliorate the security in MANETs.

A novel public key management service called Trustworthy Key Management for Mobile Ad Hoc Networks (Ad Hoc TKM) suggested by Johann van der Merwe et al. [15] extracts the best of the threshold cryptography and certificate chaining and amalgamates it with the self-certified public keys and self-certificates to fabricate a key management service guarantying security that is trustworthy and readily available to the users.

Wu et al. [16] contemplated attacks on MANETs and their countermeasures on protocol layer wise criteria. In their work, a detailed examination of recent attacks, such as flooding, black hole, link withholding, link spoofing, replay, wormhole, and colluding miserly, as well as their countermeasures were reported.

In references [17] and [18] an overview of secure routing protocols (Authenticated routing for ad hoc networks (ARAN), Secure AODV (SAODV) [19], Secure Efficient Ad hoc Distance vector routing protocol (SEAD), Secure Routing Protocol (SRP), and Secure Link-State Protocol (SLSP) in MANETs were discussed.

Madhavi [20] suggested IDS for mobile ad hoc networks that can capture the assurance of nodes receiving the fair quota of the transmission channel. The system reckoned on overhearing the packet transmission of neighboring nodes that made it an efficacious system in networks with nodes having inconsistent transmission power and directional antennas for different neighbors. The threshold can be reduced dynamically by the proposed system, which is independent of any of the immune system features that are adapted to apply in this approach.

Capkun et al. [21] proposed a certificate-predicated public key management in which the nodes contribute pairs of their own public and private keys with the certificate of the public key assembled together a confined validity period to deal with the network partitions in MANETs. The process of seeking a valid certificate chain triggers a communication overhead. Careful consideration of the explicit key revocation requires a high communication overhead while security susceptibility is caused by implicit key revocation until the private key compromise is explored.

Boudec and Sarafijanovic in [22] mapped a body as the MANET and classified it as well behaved nodes and misbehaving nodes, and the antigen as self-cells, non-self-cells, and a flow of observed DSR protocol. In the offline learning phase, Negative Selection and Bone Marrow Antibodies were constructed, and the network with only certified nodes was imitated as bone marrow where the B cells maturated in the immune system.

Huang and Wu [23] showed a certificate path revelation algorithm for MANETs premised on the hierarchical PKI structure that makes use of multiple CAs lacking concrete trust framework. Huang and Nicol [24] reported that the shortest certificate chain fails to predict the most trustworthy path for grasping the public key of a

target node. The reason behind this is that the trustworthiness observed in each intermediate node differs on the certificate chain. Vinh et al. [25] implanted a group header for public key management in a group communication system, where the group header is culled based on trust.

As the security for ad hoc network is a challenging issue, existing solutions have failed to solve the security issue and the missing factor is an innovating an effective mechanism that can frame a rationale inference by considering the available knowledge with the inclusion of an intrusion detection result, prior experience, communication data value, and preferences, to evaluate the trust relationship among network nodes. From the evaluation result, an approximately correct decision on security protection routing can be formulated by the adaptation of the special characteristics of the mobile ad-hoc networks for the upcoming technology.

3. Proposed TPR Framework with Optimized Cluster Head

This section elaborates the system design and methodology, which concerns its ultimate design and the features of proposed framework. Fig. 1 views the overall system design of the proposed framework. The proposed framework comprises a Trust Predicated Routing Framework for secure routing with an optimized cluster head selection using the Cuckoo search algorithm. Primarily, the initial cluster head selection is performed based on the prior history of energy and trust levels of the nodes maintained by the trust authority. Subsequently, cluster formation is carried on through cluster head by accepting the control messages sent from the mobile nodes in the network. The TPR framework can be proposed for secure path routing through cluster formation in the MANET. During the routing process, energy drops usually occur in the cluster head due to the heavy work load in the node, leading to re-clustering of the cluster group and a selection of another cluster head to avoid packet loss during data transmission. The re-clustering process exhibits a hindrance for the overall efficiency of the routing process and consuming time. This paper proposes an optimized algorithm Cuckoo search in this framework that selects the secondary cluster head within the initially formed cluster group and eliminates the need to re-cluster the cluster formation. The detailed functionality is narrated in the upcoming subsections.

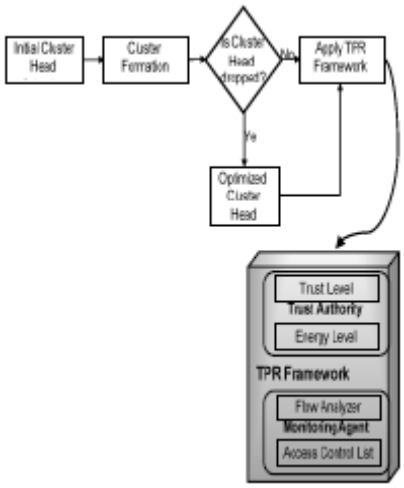

Fig. 1. System Design of Proposed TPR Framework with Optimized Cluster Head.

Consider a mobile ad hoc network with N number of nodes with their prior history of energy and trust levels. The trust authority perpetuates the past history of the nodes and updates the energy and trust levels for every routing process carried out by the network. Monitoring Agent (MA), which is a table maintained in the proposed framework, has a FA (FA) for monitoring the traffic in the network. Whenever the packet enters the network it should ensure the Access Control List (ACL) for further progress in the network. The tables' trust authority and monitoring agent way of working are expounded below.

3.1 Trust Authority

In the proposed TPR framework, MANET makes use of a trust authority that resides on the MANET nodes. Each node maintains its trust level and energy level individually by following the Trust Authority. Based on the events, such as the discovery of network loops and the prior history, the trust level of each neighbor is maintained by the Trust Authority.

The Trust Authority also maintains the energy levels of each node to efficiently calculate the energy level of the nodes in MANET. Information regarding the Trust level values is provided in the following subsections.

3.1.1 Trust Level Calculation

The reflection of the trust level can be shown in the parameters: reliability, utility, availability, reputation, risk, confidence in addition to quality of services of a node. On the other hand, trust level cannot be redefined exactly in the above said concepts. The reason behind this is that the trust level is an abstract concept, which combines many complicated factors. Initially, all the nodes in the network are labeled with the trust level of an unknown. The average trust level of a node can be captured from the neighboring nodes' report of the corresponding node. In this way, a simple, logical calculation towards aggregating trust levels of the nodes can be made. The trust level calculation from node a about node b, T_L as a weighted sum of its own trust (monitor) and the recommendations of neighbors can be illustrated in the fundamental equation as follows:

$$T_L = (1-\alpha)E + \alpha.R + P \tag{1}$$

where

E : Energy level of the node
P : Packet length of the node
R : Aggregate recommendation of the neighbor
α : is a parameter that allows thee nodes to choose the most relevant factor, and ranges from [0, 1].

3.1.2 Energy Level Calculation

A periodic energy level calculation of every node in the mobile ad hoc network can be performed taking the parameters as the power consumption and the total energy of the nodes. The operation of each node in the network can be in either transmission mode or reception mode

In transmission mode, the energy consumption of a node is given by,

$$E_c = e_t \times T \ , \tag{2}$$

where e_t is the transmitting energy, T is the transmission time and E_c is the energy consumption.

In the same way, the energy consumption in the reception mode is:

$$E_c = e_r \times T \tag{3}$$

where e_r is the reception energy and T is the reception time. Eq. (4) shows the way of calculating the value of T.

$$T = \frac{D_s}{D_r} \tag{4}$$

where D_s is the data size and D_r is the data rate.

Finally, using Eqs. (2) and (3), the energy level of the node is calculated as,

$$Energy\ Level(E_L) = E_i - E_c \tag{5}$$

where E_i is the initial energy of the node.

Initially, all nodes in the network are charged with 100% battery power that can be taken as the initial energy of the node. When the data is transmitted and received, the energy level is decreased based on Eq. (5). A drop in the energy level of the node below 40% indicates that the particular node cannot act as a router to forward the packets.

3.2 Monitoring Agent for Traffic and Flow Control

The Flow Analyzer (FA) maintained by the Monitoring Agent (MA) for monitoring the traffic in the network for assuring the Access Control List (ACL) whenever the packet enters the network for further progress in the network. The main purposes of the FA and access control list are given in the following subsections.

3.2.1 Flow Analyzer

The tedious task in the network is traffic flow monitoring that is performed by the FA, which snatches the transmission of the packets between two nodes in MANET. The FA considers the fidelity value and the ID of the specific node to determine the congestion that occurs in the transmission path of packet flow.

In the TPR framework, the FA performs the optimized functionalities that contribute to the efficiency of the underlying network. The FA collects the traffic flow information between the source and destination and forwards the information to the monitoring interface. The FA also takes responsibility for sampling the information regarding traffic flow, preparing a record to indicate the flow terminology. The next function of FA is to promulgate the filtered traffic to divergent packet analyzers, retrieving the original format of data. In addition, it can eradicate the undesirable traffic and record the unwanted list.

The traffic congestion can be evaluated by the FA based on the above mentioned functions in the requested routing path and devises a path status message as *Busy* or *Free*. The path status message *Busy* indicates stopping of the transmission process and wait for the status message as *Free*. Upon its completion, the FA allows the ACL for further level security routing.

3.2.2 Access Control List (ACL)

The Access Control List (ACL) is a filter that enables control of the routing updates apart from providing forwarding permission of the packets in or out of a MANET. The network administrators categorically utilize ACL to filter the traffic and provide extra security for their networks and can be applied to the MANET nodes.

In the access control list (ACL), once a packet arrives at the node, certain information extraction of the nodes from the packet header is fabricated and decisions as to whether the packet can pass through or to be dropped based on the source and destination IP addresses, source port and destination port, and the protocol of the packet are made according to the filter rules.

The formulation of a cluster as well as the initial cluster head selection is explained in the following sections, in which the processes are very important for reducing the transmission collision and time preservation in routing.

3.3 Clustering for Reduced Transmission Collision

Clustering is an auspicious approach for framing hierarchies and simplifying the routing process in mobile ad-hoc network environments. The mobile nodes in the MANET are divided into several virtual zones called as cluster groups in the clustering structure. The mobile nodes in the network may be assigned a different status or function, such as the cluster head, cluster gateway, or cluster member. From the cluster head, knowledge of the particular cluster group can be obtained and the cluster head can act as a coordinator of the cluster operations. The cluster gateway can be formed by choosing the Boarder node in the communication range for more than one cluster group. The summarization of cluster information is sent to the neighboring cluster heads via the gateways.

3.3.1 Initial Cluster Head Selection

The principal objective of clustering is to identify opportune node representatives, i.e. cluster heads (CHs), to store the routing and topological information and to maximize the cluster stability. In the proposed framework,

Algorithm 1. Joining of new nodes in Cluster.

```
/* The neighboring nodes send 'Status' to new node*/
    if (clusterhead(n) = TRUE) then
    status := cost n;
    else
    status := clusterhead(n);
    end if;
    send status(n,d);
```

the formation of initial cluster head will be based on the past history of the mobile nodes present in the trust authority. The energy level and trust level of each and every node is maintained and the entire process is performed based on the past history which contains the energy level and the trust level of the nodes in the network. The power consumption of the cluster heads is more than the other nodes as they have other special roles such as coordinators of the clustering process and relaying routers. The initially node with a high energy and trust level can be chosen as the cluster head from the given network model. When the energy level is the same for more than two nodes, the node with the highest trust level will be crowned as the initial cluster head. The calculation of the energy and trust level was explained in subsections 3.1.1 and 3.1.2.

3.3.2 Cluster Formation

In the proposed framework, the cluster formation process was carried out based on the selection of the initial cluster head. Adding a node to the cluster group mingles the added node as the cluster member of the specific cluster group. The inclusion of a new node in the cluster group can be based on four control messages *Hello, Status, Join* and Acknowledge messages, which required for cluster group authentication. Primarily, the presence of a new node *d* is indicated by sending a *Hello* message by the new node. On the receipt of the *Hello,* a *Status* message is forwarded to the node by all the surrounding neighbors of node *d* as a response. Cluster head *n* can be identified by node *d* by checking the cost value mentioned in the status message. If not, the *Status* message contains the *ID* of its cluster head node, showing that the neighbor node *n* is a cluster member. Algorithm 1 illustrates the joining process of a new cluster member to the particular cluster group.

3.3.3 Cluster Set Table

The movement of the mobile nodes in MANET is arbitrary; hence, the nodes in the cluster may drop frequently and randomly at unpredictable times, resulting in unidirectional as well as bidirectional links. Based on the network mobility, the nodes can go beyond the transmission range of their cluster head, crossing the border and stepping into another cluster, changing its neighborhood, resulting changes in the number of clusters and number of nodes in a cluster group. Based on the mobility of the nodes, the inclusion of new nodes in the cluster and dropped nodes from the cluster will be maintained in the cluster set table.

Cluster Number	Cluster Head	Nodes in Cluster	Newly Added Nodes (per every routing request)	Dropped Nodes (per every routing request)
1	C	A, B, E, F	D, G	F
2	H	L, N, O	M, J, I	L
3	X	W, U, Y, Z	V, P, Q, R, S	W, Y

Fig. 2. Example of a Cluster Set Table.

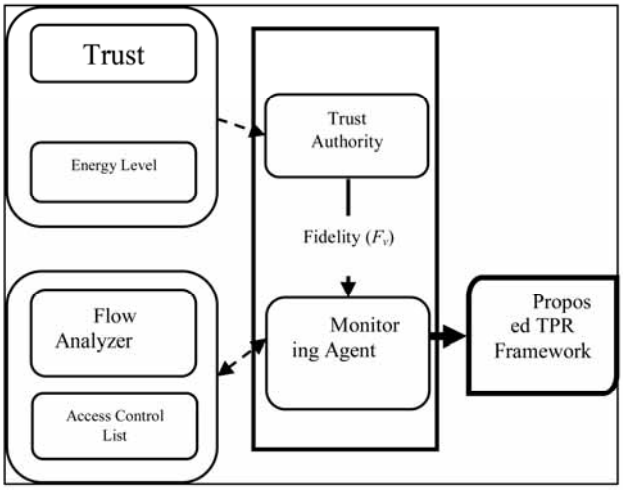

Fig. 3. System model for the proposed TPR framework.

In Fig. 4, samples of the cluster set are presented indicating the cluster number, cluster head and nodes present in the particular cluster group. The nodes present in the cluster group will be changed alternatively in the cluster set table based on the fact that newly added and dropped nodes from the cluster group are updated for every routing request in the network.

3.4 Proposed TPR Framework

Upon successful completion of initial cluster head selection and cluster formation, the Trust Predicated Routing (TPR) framework will be used for secure routing path selection in mobile ad-hoc networks. Trust establishment in a MANET prefers significant detection of intruders and isolating them promptly to avoid exploitation of any network resources but relying only on self-detecting misbehaviors, drags to an erroneous evaluation of trust. In fact, selfish nodes cannot be detected by a node that is authentically not sending any packets currently in its neighborhood. As a consequence, fraternization between the neighboring nodes becomes vital. In the proposed scheme, the behavior of every node is monitored by its neighbors, and upon the detection of any aberrant action from any of them, it broadcasts this information to the other nodes to make them vigilant about its observation. Fig. 5 presents the overall system model of the proposed

TPR framework.

In the proposed TPR framework the performance enhancement increases by making use of the trust authority that resides on the MANET nodes. A data structure called the trust authority is maintained for storing the trust and energy levels of every node in the network and is updated for every routing process in the network.

fidelity value can be calculated based on the trust and energy levels of the nodes in the trust authority. In MANET, the fidelity value calculation is a promising approach to ensuring cooperation and fairness. The fidelity value is calculated based on three decision values, which are required in both the energy and trust level values, and they are high, medium and low according to their declared high threshold value and low threshold value in the energy and trust levels. The trust level decision value calculation using threshold values are given as follows:

$$D_T = \begin{cases} High;\ if\ T_L \geq Th_T \\ Medium;\ if\ Th_T > T_L \geq Tl_T \\ Low;\ if\ T_L < Tl_T \end{cases} \quad (6)$$

where DT is the trust level decision value, ThT and TlT are the high and low level threshold values of the trust level.

The conditions for energy level decision values, DE, depends on the energy level threshold value as follows:

$$D_E = \begin{cases} High;\ if\ E_L \geq Th_E \\ Medium;\ if\ Th_E > E_L \geq Tl_E \\ Low;\ if\ E_L < Tl_E \end{cases} \quad (7)$$

where Th_E and Tl_E are the high and low energy level threshold values. The threshold values of both the trust and energy levels may be miscellaneous contingents of the security specifications of each progressing chore that are given in Eqs. (6) and (7).

The following six rules resolve the fidelity value based on the decision values obtained from Eqs. (6) and (7).

Rule 1: The fidelity value is extremely high if the decision value of trust and energy level is high.

Rule 2: The fidelity value is very high if the decision value of the trust level is medium and the energy level is high.

Rule 3: The fidelity value is high if the decision value of the trust level is high and energy level is medium

Rule 4: The fidelity value is medium if the decision value of the trust and energy level is medium.

Rule 5: The fidelity value is low if the decision value of the trust level is low and the energy level is medium.

Rule 6: The fidelity value is very low if the decision value of the trust level is anything and decision value of energy level is low.

The conformity of the node regarding energy and trust is revealed using the fidelity value (Fv), which can be calculated based on abovementioned six rules.

Trust Predicated Routing in the proposed architecture has two possibilities when the source node S wants to send data to the destination node D, in which the First option is both the source and destination are available in the same cluster, as explained in Algorithm 2. On the other hand, the source and destination are present in separate clusters, as

Algorithm 2. Routing for the Source and Destination are in the Same Cluster.

If source and destination are in the same cluster:

{Source node S Broadcast RREQ message;

Cluster head received the RREQ message;

Then checks the fidelity level of source node;

If fidelity level of source node is acceptable by CH}

{Re-broadcasts the RREQ within the cluster with destination ID;

When RREQ reach the destination,

The destination return a RREP with fidelity value and route traffic details}

{If CH received RREP

Check fidelity value,

If fidelity = low,

Discard the message}

Else

{Check traffic congestion through monitoring agent;

If the ACL has destination node id,

Then accept the RREP and allow the data to send}

Algorithm 3. Routing for the Source and Destination are in the Same Cluster.

If source and destination are in different clusters:

{Source node S Broadcast RREQ message;

Cluster head H received the RREQ message;

Then checks the fidelity level of source node;

If fidelity level of source node is acceptable by CH}

{Checks the cluster of the destination;

Initiate cluster set table,

Find the cluster and cluster head}

{Broadcasts the RREQ to cluster through cluster gateway;

When RREQ reach the CH,

Then checks the fidelity level of intermediate nodes;

If fidelity level of intermediate nodes are acceptable by CH}

{CH Re-broadcasts the RREQ within the cluster with destination ID;

When RREQ reach the destination,

The destination return a RREP with fidelity value and route traffic details}

{If CH received RREP

Check fidelity value,

If fidelity = low,

Discard the message}

Else

{Check traffic congestion through monitoring agent;

If the ACL has destination node id,

Then accept the RREP and allow the data to send}

Algorithm 4. Pseudo Code for the Cuckoo Search optimization algorithm.

```
begin
Objective function f(x), x = (x1,.....,xd)^T
Generate initial population of n host nests xi(i= 1,2,….,n)
While (t < MaxGeneration) or (stop criterion)
    Get a cuckoo randomly by Levy flights
        Evaluate its quality/fitness Fi
    Choose a nest among n (say j) randomly
    If Fi > Fj
        Replace j by the new solution;
    end
    A fraction (pa) of worse nests are abandoned and new ones are built;
    Keep the best solutions or (nests with quality solutions);
    Rank the solutions and find the current best
End while
Post-process results and visualization
end
```

expressed in Algorithm 3. Coordinators of the clustering process and relaying routers play significant roles in both of the two routing frameworks cluster head so the node in the cluster head consumes spare energy compared to the other nodes, which affects the routing procedure. This leads to re-clustering of the group using the conventional secure routing approaches that elects another cluster head for avoiding the packet loss during data transmission. The problem is that the overall efficiency of the routing process is reduced and the processing time is increased. There is no need to re-cluster the group using the proposed Cuckoo search based optimization algorithm, which selects the secondary cluster head within the initially formed cluster group to overcome the problem. The following subsections provide a detailed explanation of the optimized cluster head.

3.5 Cuckoo Search Algorithm for the Optimized Cluster Head

The Cuckoo search based optimization algorithm is furnished with the proposed routing framework because of its specialty in quality and precision of the global optimal solution for the optimized secondary cluster head selection.

Algorithm 4 presents the pseudo code for cuckoo search written in a biased way with random step sizes. Eqs. (8)-(10) gives cuckoo search's biased random step size that can be determined as follows.

$$stepsize = rndval * (nest(rnd(n)) - nest(rnd(n)) \quad (8)$$

$$New\_nest = nest + stepsize*K \quad (9)$$

where

n : number of host nests

rnd : random value

$$K = rand(size(nest)) > p_a \quad (10)$$

The flow chart Fig. 6 illustrates the cuckoo search based cluster head optimization and the detailed processing

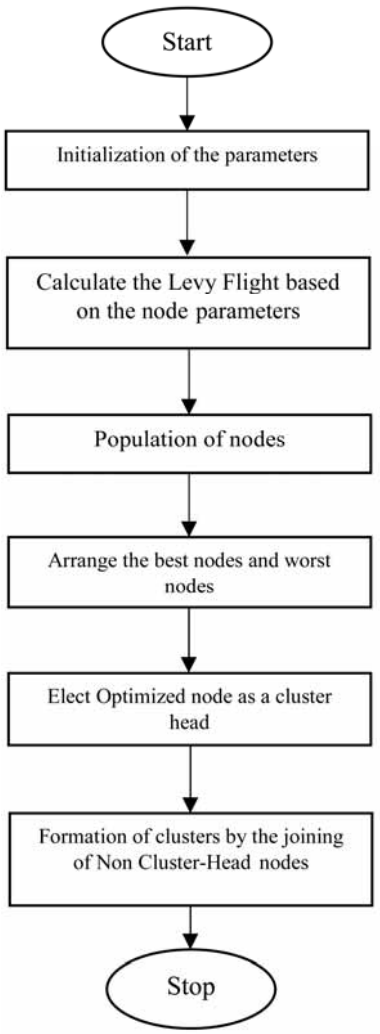

Fig. 4. Flowchart of cuckoo search based optimization algorithm.

steps for obtaining the optimized cluster head are given as follows.

Step 1: Initialization

Assume the number of mobile nodes and node parameters as cuckoo nests and eggs in the nests to start the search in which multiple eggs in each nest represents a set of solutions. Consider N number of nodes in the network and initialize the trust level and energy level of nodes in the mobile ad hoc network where, T and E are the trust level and the energy level of the nodes, respectively.

Step 2: Calculation of Levy Flight

The random step length is determined from a Levy distribution when the Levy flight contributes a random walk

$$Levy \sim u = t^{-\lambda} \; ; (1 < \lambda \leq 3) \quad (11)$$

The Levy has an infinite variance and mean that essentially form a random walk process with a power law step length distribution and a heavy tail around the optimal solution obtained so far, which generates some new solutions that will speed up the local search.

The Levy flight is calculated with two maverick random variables, T and E, which have a normal Gaussian distribution from this nonlinear transformation.

$$v = T / |E|^{\frac{1}{\beta}} \tag{12}$$

The Following equation shows the sum of variables within the nonlinear transformation with an appropriate normalization.

$$z_n = \frac{1}{n^{\frac{1}{\beta}}} \sum_{k=1}^{n} v_k \tag{13}$$

Eq. (13) converges on the Levy probability distribution of a larger n where, β represents the step size function.

Step 3: Population of Nodes

In the beginning of the population process n number of nodes are created randomly without violating the node parameters T and E. The following equation shows the generation of new population solutions $x^{(t+1)}$ for the next generation,

$$x_i^{(t+1)} = x_i^t + \beta \oplus Levy(\lambda) \tag{14}$$

where $\beta > 0$ is the step size and $\oplus$ means entry wise multiplication.

Set the initial minimum cost value for all the nodes in the network and evaluate the initial population cost using the cost function J(θ) for the node. Update the population value of nodes in every search process.

Step 4: Best and Worst Nodes

A queue is formed by sorting the best and worst nodes depending on the population of nodes and Levy flight values, in which the best nodes are conveyed to the next generation with a high quality of node parameters that are determined using the probability function Pa. On the other hand, the worst nodes are discovered and discard from further calculations.

Step 5: Optimized Node as a Cluster Head

The highly optimized node that has highly recommended node parameters from the sorted queue will be elected as the cluster head for the particular cluster group, which means the trust and energy level of the cluster head node will be sufficient for treating the collision free routing.

4. Experimental Results

By incorporating the idea of the TPR framework, a more pliable and less overhead secure routing protocol for MANETs can be established.

Matlab R2013a was used to assess the TPR framework in a mobile ad hoc network environment for substantially evaluating the performance of ad-hoc routing protocols. The package naturally models random node mobility and physical radio propagation effects, such as signal strength, interference, capture effect, and end to end delay. The simulator implements the complete IEEE 802.11 standard Medium Access Control (MAC) protocol at the link layer.

4.1 Performance Parameters

The proposed TPR framework can be assessed by making a comparison with the Ad-hoc On Demand Vector Routing protocol (AODV) [26]. The results showed that both protocols run on identical movements and communication scenarios. The metrics for the performance evaluation used for the comparison process is given below.

Routing Message Overhead: Based on the total number of control packets transmitted, the Routing message overhead was calculated. As there is an increase in the routing message overhead, the performance of the ad-hoc network decreased dramatically as it consumes portions from the bandwidth available for data transfer data between the nodes.

Throughput: The modification performance can be evaluated by considering the important parameter throughput that can be calculated as the number of bits received per second. The throughput can be affected based on the total number of packets dropped or left waiting for a route that can be calculated by adding the number of packets dropped or waiting for a route considering all the nodes.

End-to-end delay: End-to-end delay deals with the time taken by a packet to reach a destination from the source through the network.

Packet Deliver Ratio: It can be defined as the ratio of the number of packets that are delivered successfully to a destination to the number of packets that have been sent out by the sender node.

Energy Consumption: Energy consumption deals with the total consumption of energy or power of a node in the network.

4.2 Simulation Scenarios

An evaluation of the simulated FPR framework can be done by comparing three different scenarios. The first scenario is the 40 nodes scenario on a rectangular area of 800*200 m2. The second scenario is an 80 nodes scenario on a rectangular area of 1000 * 400 m2. The third scenario is a 100 nodes scenario on a rectangular area of 1500 * 600 m2. The rectangular area forces the nodes to establish longer routes and by making use of that, the effect of the proposed framework can be studied. This scenario denotes the small size ad-hoc networks and different ad-hoc applications make use of the network size information, such as conferencing, Emergency services where there is no infrastructure, and search and rescue operations.

4.3 Scenarios Results

The following subsections show the results of the simulation scenarios for the various number of nodes in the mobile ad-hoc network.

Routing Message Overhead

Fig. 5 shows the routing message overhead caused from both AODV and FPR routing protocols. The FPR

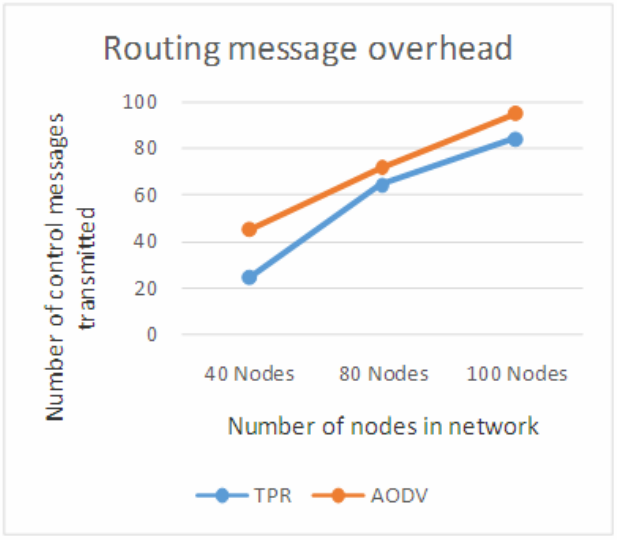

Fig. 5. Routing Message overhead for proposed and AODV protocol.

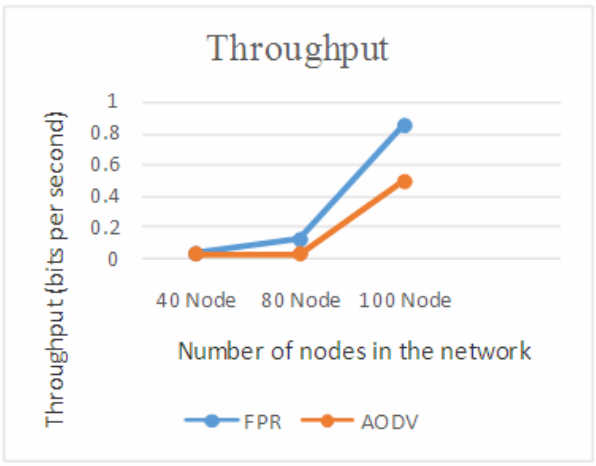

Fig. 6. Throughput for proposed and AODV protocol.

routing message overhead is an average of 20% lower than the AODV routing message overhead. The result also illustrates the outcome of the FA and access control list on reducing the routing message overhead.

Throughput

Fig. 6 shows the throughput from both TPR and AODV. The TPR has a higher throughput than AODV routing protocol by 5.6% on average, which is a small increase. This shows that the effect of the TPR framework does not appear in small sized networks.

End to End Delay

The end-to-end delay results show that the TPR Framework delivers packets with less delay than the AODV in most the scenarios considered for the simulations in Fig. 7. The delay is significantly lower in the 40 and 100 node network configuration. In both the large and small nodes scenario sets, the delay shown by FPR is at least 190 ms lower. In the larger 80 node

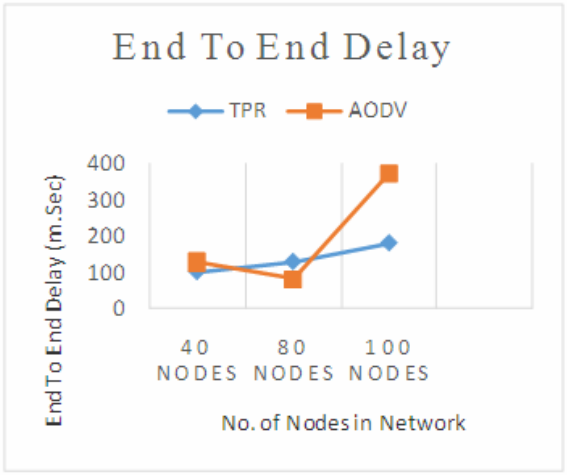

Fig. 7. End-to-End Delay for proposed and AODV protocol.

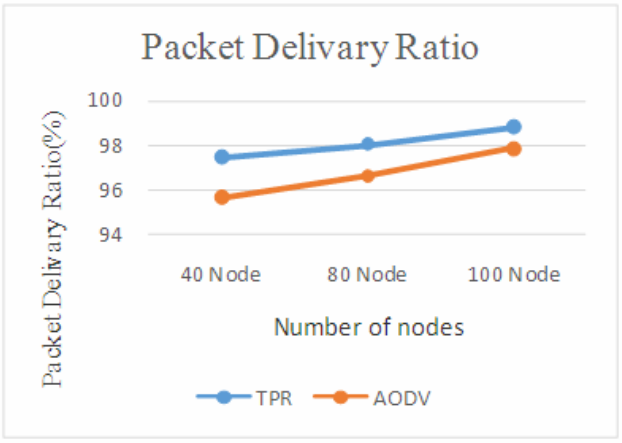

Fig. 8. Packet Delivery Ratio for the proposed and AODV protocol.

network, the proposed system delay value is higher than the AODV protocol.

Packet Delivery Ratio

Fig. 8 shows the packet delivery ratio results for the two different security protocols of proposed TPR framework and conventional AODV protocol. The packet delivery ratio decreases at high speeds because both protocols drop packets when there is considerable topology change and the links to next hops are consistently broken. The curves for the two protocols display a similar shape, which is expected due to similarities in their operations. On the other hand, the proposed protocol's delivery ratio is consistently better than the AODV in all sets of nodes in the network.

TPR's packet delivery ratio results have a particular advantage over AODV in all sets of node network configuration. An at least 3% gap in the packet delivery ratios can be achieved by the two protocols with varying number of nodes in the network. The routing of the network traffic by the shortest-path AODV algorithm creates congestion at certain nodes in the network. The

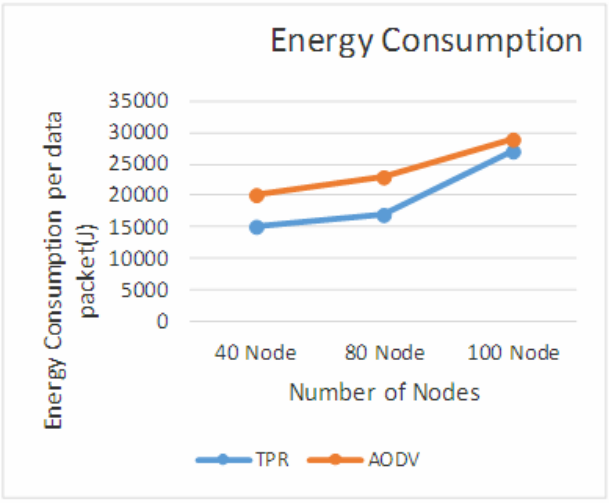

Fig. 9. Energy consumption for the proposed and AODV protocol.

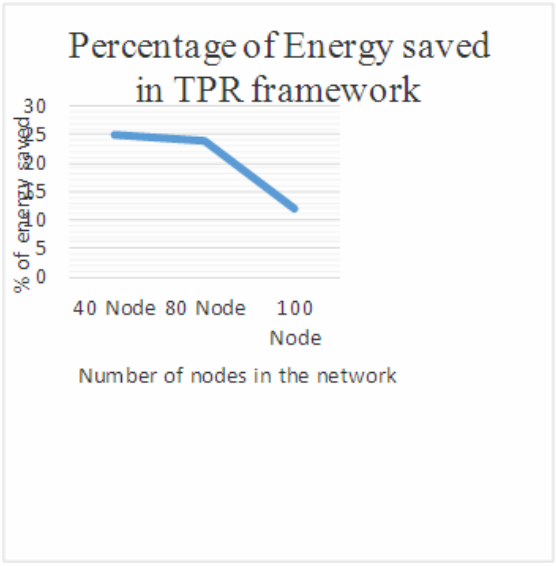

Fig. 10. Percentage of energy saved in the proposed framework over the AODV protocol.

protocol queues of the routing agents have limited capacity, and the packets are dropped when overloaded. Because TPR avoids the creation of such congestion scenarios, the dropping of packets from overloaded protocol queues is reduced significantly.

Energy Consumption

Fig. 9 shows the energy spent per data packet for the TPR framework and AODV protocol. The energy consumption per data packet is always lower in the TPR framework compared to AODV protocol. The energy consumption per data packet increases in both the TPR framework and AODV protocol as the network size increases. The reason is that the data packets are traveling more hops in both protocols when a larger network size is used.

Fig. 10 compares the percentage of energy saving in the TPR framework compared to AODV protocol. The energy saving is a maximum when the network size is small, which is almost 25% when the network has 40 nodes. That saving in energy decreases with increasing network size. When the network has 100 nodes, the energy saving in the TPR framework is almost 12%.

6. Conclusion

In today's scenario, the number of ad hoc networks is increasing continuously. Most researchers concentrated mainly on routing issues and scarcely on sundry attacks. On the other hand, there is a desideratum of a resilient system that can operate felicitously in the presence of malevolent activities. Therefore, there is increasing need for trust establishment. Some studies have been conducted in this area but no model is sufficient to provide a consummate framework. Moreover, it is more difficult to ascertain that the security implementation conforms to the global framework and there are certain link failures in the network.

This paper proposed an incipient approach based on trust-predicated routing (TPR) framework. Only few studies have been done in this field. Trust Predicated Routing Framework for secure routing with an optimized cluster head selection using the Cuckoo search algorithm is proposed. PR framework provides full security and reliability for the proposed routing protocol and the Cuckoo search algorithm reducing the time consumption and delivers efficient routing process by selecting the optimized secondary cluster head without re-clustering the whole cluster group. The simulation showed that the proposed framework achieves a high packet delivery ratio and throughput with a low end-to-end delay, routing message overhead and energy consumption.

References

[1] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang and Nei Kato, "Cluster-based Certificate Revocation withVindication Capability for Mobile Ad Hoc Networks", IEEE Transactions On Parallel And Distributed Systems, vol.24,no.2,pp.239-249,2013. Article (CrossRef Link)

[2] Sevil Sen, John A.Clark and Juan E.Tapiador, "Security of Self-Organizing NetworksMANET, WSN, WMN, VANET", Auerbach Publications, 2010, 978-1-4398-1920-3. Article (CrossRef Link)

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, vol.40, no.10, pp.70-75, 2002. Article (CrossRef Link)

[4] Wensheng Zhang, R. Rao, Guohong Cao and George Kesidis, "Secure Routing In Ad Hoc Networks and A Related Intrusion Detection Problem", IEEE Military Communications, vol.2, pp.735-740, 2003. Article (CrossRef Link)

[5] Anand Patwardhan, Jim Parker and Anupam Joshi, "Secure Routing and Intrusion Detection in Ad Hoc Networks", IEEE Pervasive Computing and

Communications, PP.191-199, 2005. Article (CrossRef Link)
[6] Martin K Parmar and Harikrishna B Jethva, "Survey on Mobile ADHOC Network and Security Attacks on Network Layer", International Journal of Advanced Research in Computer Science and Software Engineering, vol.3, no.11, pp.708-716, 2013.
[7] Yashar Najaflou, Behrouz Jedari, Feng Xia, Laurence T. Yang and Mohammad S. Obaidat, "Safety Challenges and Solutions in Mobile Social Networks", IEEE Systems Journal, no.99, pp.1-21, 2013. Article (CrossRef Link)
[8] Ghanshyam Prasad Dubey, Prof. Amit Sinhal and Prof. Neetesh Gupta, "Network Performance investigation in Presence of Multiple Vital Node and IDS in MANET", International Journal of Computer Science and Information Technologies, vol.3, no.3, pp.3879-3883, 2012. Article (CrossRef Link)
[9] A.Jayanand and Prof.Dr.T.Jebarajan, "Performance Investigation and Analysis of Secured MANET Routing Protocols", International Journal of Computer Science and Information Technologies, vol.3, no.2, pp.3512-3516, 2012. Article (CrossRef Link)
[10] Suman Deswal and Sukhbir Singh, "Implementation of Routing Security Aspects in AODV", International Journal of Computer Theory and Engineering, vol.2, no.1, pp.135-138, 2010. Article (CrossRef Link)
[11] Yih-Chun Hu, David B. Johnson and Adrian Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", Elsevier B.V. Ad Hoc Networks, vol.1, pp.175-192, 2003. Article (CrossRef Link)
[12] Yih-Chun Hu and Adrian Perrig, "A Survey of SecureWireless Ad Hoc Routing", IEEE Security & Privacy, vol.2, no.3, pp.28-39, 2004. Article (CrossRef Link)
[13] Levente Buttyan and Ta Vinh Thong, "Formal verification of secure ad-hoc network routing protocols using deductive model-checking", IEEE Wireless and Mobile Networking, pp.1-6, 2010. Article (CrossRef Link)
[14] V.Balakrishnan, V.Varadharajan, et al. "Fellowship: Defense Against Flooding and Packet Drop Attacks In MANET," Network Operations and Management Symposium, NOMS 2006, pp. 1- 4, 2006. Article (CrossRef Link)
[15] Johann van der Merwe, Dawoud, *et al.* "Trustworthy Key Management for Mobile Ad Hoc Networks", ACM Computing Surveys (CSUR), Volume 39, Issue 1, 2007. Article (CrossRef Link)
[16] B.Wu, J.Chen, *et al.* "A Survey of Attacks andCountermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006. Article (CrossRef Link)
[17] D. Wang, M. Hu, H. Zhi, "A Survey of Secure Routing in Ad Hoc Networks," IEEE Ninth International Conference on Web-Age Information Management, 2008, (WAIM '08), pp.482-486, July 2008. Article (CrossRef Link)
[18] K.Sanzgiri, D.LaFlamme, *et al.* "Authenticated Routing for Ad Hoc Networks," Proceedings of IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, March 2005. Article (CrossRef Link)
[19] Y.C.Hu, A.Perrig, *et al.*"Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom'02, Atlanta, GA, pp. 12-13 September 2002. Article (CrossRef Link)
[20] S. Madhavi, Dr. Tai Hoon Kim, " An intrusion detection system in mobile Ad hoc networks", International Journal of Security and Its Applications Vol. 2, No.3, July, 2008. Article (CrossRef Link)
[21] S. Capkun, L. Buttya, *et al.*"Self-organized public-key management for mobile ad hoc networks," IEEE Transactions on Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan. – Mar., 2003. Article (CrossRef Link)
[22] Yasir Abdelgadir Mohamed*, Azween B. Abdullah, "Security Mechanism For MANETS",Journal of Engineering Science and Technology, Vol. 4, No. 2, pp: 231 – 242,2009. jestec.taylors.edu.my/.../Vol_4_2_231-242_YASIR%20ABDELGADIR..
[23] H. Huang and S. F. Wu, "An approach to certificate path discovery in mobile ad hoc networks," 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Oct. 2003. Article (CrossRef Link)
[24] J. Huang and D. Nicol, "A calculus of trust and its application to PKI and identity management," ACM 8th Symposium on Identity and Trust on the Internet, Gaithersburg, MD, USA, April 2009. citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.210.3881
[25] N. V. Vinh, M.-K. Kim, H. Jun, and N. Q. Tung, "Group-based public-key management for self-securing large mobile ad-hoc networks," Int'l Forum on Strategic Technology, pp. 250-253, Oct. 2007.
[26] Hua Yang and Zhi-yuan Li, "Simulation and analysis of a modified AODV routing protocols", Computer Science and Network Technology (ICCSNT), vol. 3, pp. 1440 – 1444, 2011.

J. Chandra Sekhar, M.Sc. (Computer Science), M.Tech.(CSE) is working as an Associate Professor in the Department of CSE, Chalapathi Institute of Technology, Guntur, A.P. He is a Ph.D. Research Scholar in the Department of CSE, Acharya Nagarjuna University, Guntur A.P. He is having 10 years of experience in Teaching.

Ramineni Sivaram Prasad, Ph.D. is working as an Associate Professor & Research Director In Department of CSE, Acharya Nagarjuna University, Guntur A.P. He has published more than 80 Research papers in both National and International journals, attended 104 seminars, has given several extension lectures, and published 5 books to his credit.