EAI Endorsed Transactions
on Energy Web
Research Article EAI.EU

Secure Group based Routing and Flawless Trust Formulation in MANET using Unsupervised Machine Learning Approach for IoT Applications

Maitreyi Ponguwala[1],* and DR.Sreenivasa Rao[2]

[1]Research Scholar of JNTUH, MGIT Hyderabad, India, Ponguwalamaitreyi@gmail.com
[2]Professor in Dept. Of CSE, JNTUH Hyderabad, India, Srmeda@jntuh.ac.in

Abstract

INTRODUCTION: Mobile Adhoc Network (MANET) is integrated with Internet of Things (IoT) in many application cases due to its flexibility and scalability. The dynamic nature of MANET introduces some security threats in IoT environment. In those threats, Blackhole attack and Grayhole attack are severe routing attacks that disrupts routing algorithm to crack transmission in the entire network.
OBJECTIVES: Many security mechanisms are introduced in MANET based on trust computation schemes. However, computation of inaccurate trust value degrades the performance of mitigation schemes. Thus the major objective of this work is to design a novel security mechanism to protect the MANET-IoT from different adversaries.
METHODS: in this paper we propose a novel group based routing algorithm with recommendation filtering supported by security monitors (SMs). Unsupervised machine learning algorithm is adapted for the purpose of recommendation filtering in the network. Initially the entire network is grouped by Secure Certificate based Group Formation (SCGF) algorithm. In each group, Recommendation Filtering by K-means algorithm (RF-K means) algorithm is employed to perform trust computation. For secure and optimal route selection, hybrid optimization algorithm that combines Genetic Algorithm and Fire Fly Algorithm (GA-FFA) is proposed. Data transmission is protected by novel Hash Message Authentication Code with Advanced Encryption Standard (HMAC-AES) algorithm in which hash function is integrated with cryptography function.
RESULTS: The proposed work is validated in network simulator-3 environment and the obtained results show better performance in terms of packet delivery ratio (96.3%), throughput (135kbps), delay (3.26ms), detection rate (99%), and energy consumption (8.5%).
CONCLUSION: The MANET-IoT network is secured by group formation and trust filtering approaches. Further, involvement of cryptography function ensures data security whereas hash function ensures data integrity..

Keywords: MANET, Recommendation Filtering, Blackhole, Grayhole, IoT applications.

Received on 20 March 2019, accepted on 03 August 2019, published on 09 October 2019

doi: 10.4108/eai.13-7-2018.160834

1. Introduction

MANET is an infrastructure-less, dynamic, and distributed network that has self-configurable ability [1]-[3]. MANET comprises group of mobile nodes that establish communication in an opportunistic manner. It follows an infrastructure-less architecture (i.e.) MANET doesn't lies on centralized base station or sink node. The specific characteristics of MANET are: multi-hop communication, decentralized infrastructure, dynamic topology, scalability, and short range connectivity. Rapid growth in wireless

*Corresponding author. Email: maithriponguwala@gmail.com technologies increases requirement of IoT nowadays [4], [5]. IoT can be described as a network that comprises millions of heterogeneous devices and enables communication among these smart ‘things’. Empowering opportunistic communication among IoT devices becomes significant since IoT involves with dynamic devices. In order to enable opportunistic communication among IoT devices MANET is integrated with IoT [6], [7]. Immersion of MANET in IoT brings improved connectivity through multi-hop communication and also supports high scalability. With the integration of MANET, IoT applications can be extended in military scenarios, smart city applications, waste management, and disaster management and so on. However, absence of the infrastructure and centralized control increases the presence of security threats in MANET-IoT environment [8], [31]. MANET is vulnerable to security attacks such as jamming attack, Grayhole attack, rushing attack, Blackhole attack, packet dropping attack, and Sybil attack. These attacks degrade the performance of entire network.

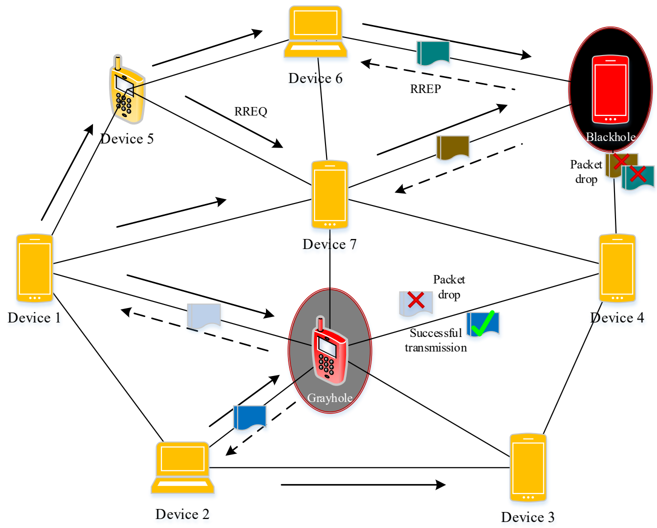


Figure 1. Blackhole and Grayhole attack in MANET-IoT

Blackhole attack and Grayhole attack are moreover similar routing attacks in MANET-IoT [9], [10]. Both attackers involved in malicious activities such as packet dropping, packet altering, packet redirecting, route alteration, and so on. In figure.1, the behavior of Blackhole attack and Grayhole attack is illustrated. Here the Blackhole attacker receives the data by sending false routing information to source node. It prevents data from reaching destination through dropping received data. This will introduce huge packet loss in the network. Similarly, Grayhole attack is a variant of Blackhole attack that drops only selective packets. In other words, the Grayhole attacker drops selective packets and forwards remaining packets to the destination. In the figure, the Grayhole attacker drops data from Device 1 and forwards the data from Device 2. Majority of Blackhole and Grayhole attack mitigation schemes utilize trust based methods for attack detection and prevention [32]. In order to mitigate Blackhole attack in MANET a data control packet and extended data routing information table (EDRI) are used in adhoc on-demand distance vector (AODV) protocol [11]. Herein routing path verification process is enabled for attack detection. Mitigation of Blackhole attack in IoT environment is carried out by securing routing protocol over low power lossy network (RPL) protocol [12]. In RPL, destination oriented directed acyclic graph (DODAG) construction is enabled with trust value computation. A flooding factor based framework for trust management (F3TM) is proposed to mitigate Grayhole attack in MANET through trust value computation [13]. For validating network nodes, a grey wolf and swarm optimizer algorithm is introduced. Cryptography schemes are also concentrated to provide security in MANET and IoT [33]. A selective significant data encryption (SSDE) algorithm utilizes Blowfish algorithm [14]. However, the cryptography technique must minimize the overhead and time consumption (i.e.) lightweight cryptography techniques are most suitable for MANET.

1.1 Major Contributions

Many research works are held on IoT and MANET in the perspective of security. But attack detection with data security and integrity is still challenging issue with the increase in number of IoT devices as well as number of adversaries in MANET-IoT environment. To cope with these issues, this paper presents following contributions,

- A novel IoT architecture is designed with the integration of MANET for establishing group based communication. A new entity namely Security Monitor (SM) is deployed in the network to strengthen the security level. Security provisioning is achieved by secure group formation, flawless trust value computation, trusted routing and partial encryption processes.
- Group formation is initialized with group head (GH) selection by SM. SCGF algorithm is proposed to form secure groups in the network. SCGF algorithm not only ensures network security but also supports dynamic mobile network management. Secure grouping process isolates unauthorized nodes in network.
- SM is responsible for flawless trust computation by using RF-K means algorithm. Unsupervised K-means algorithm is adapted for trust computation through recommendation filtering mechanism. By formulating optimal trust computation value, the Grayhole attack detection is performed.
- Trusted route selection is accomplished by effective hybrid optimization algorithm named as GA-FFA algorithm. Trusted routing process supports Blackhole attack detection through routing reply analysis. Route selection by GA-FFA algorithm is not only trustworthy but also efficient

since fitness computation involves with trust value, residual energy, link stability, and hopcount.

- Data security and integrity is achieved jointly by HMAC-AES algorithm. HMAC-AES algorithm performs based on partial encryption and partial hashing process in order to minimize encryption time and overhead without loss in security and integrity.

1.2 Paper organization

The rest of this paper is organized as follows: Section II surveys significant related works held on IoT and MANET for security provision. In section III, the problems existed in previous research works are highlighted. Section IV, details overall process of proposed security mechanism with novel algorithms. Section V, evaluates the proposed work in terms of performance metrics and compares proposed work with previous works. In section VI, we conclude our contributions and highlight the future directions of this work.

2. Related Works

In past few years, enormous numbers of research works are held on MANET and IoT for security provisioning. In this section, we provide detailed literature review on significant previous research work in order to exploit the vital challenging issues in this research area.

2.1. Survey on attack detection methods

In adhoc networks, Blackhole attack detection was performed by fuzzy based trust value computation [15]. Trust value of each node was computed in fuzzy approach based on following metrics: packet delivery ratio, percentage of energy exhaustion, percentage of buffer utilization, and number of connection requests given by a node. If computed trust value was greater than threshold value then that node is considered as normal otherwise that node is considered as Blackhole attacker. However, here node behavior analysis is performed by fuzzy approach (i.e.) threshold computation is an additional process which increases time consumption. Blackhole attack detection was performed based on dynamic threshold cumulative sum (CUSUM) test [16]. Here CUSUM test was utilized in order to detect the changes in normal behavior of AODV's sequence number. Based on AODV's sequence number (SQN), a new parameter named as Blackhole intensity was formulated for attack detection. Perhaps this method performs attack detection; this method is not able to secure transmitted data.

Blackhole attack, Grayhole attack and flooding attack were mitigated jointly by multi-level trust computation scheme [17]. Here Elliptic Curve Cryptography was used and the security was categorized into three levels. The first level computes direct trust value and indirect trust value, then in second level objective and subjective trust was computed and lastly in third level static and dynamic trust was estimated. Summing up of all the three levels of trust, the total trust value was obtained. Although ECC algorithm provides data security, it is not able to ensure data integrity which leads to data alteration. For Grayhole attack detection, denial contradictions with fictitious node mechanism (DCFM) was proposed [18]. The original DCFM algorithm was developed to mitigate node isolation attack in Optimized Link State Routing (OLSR) based routing algorithm. Then the algorithm was improved to extend the attack detection to Grayhole attack. This method was able to handle passive silent attacker, randomly located attacker, initially 1-hop neighbor attacker, shadow attacker, and man in the middle attacker. This method increases complexity while fails to improved detection accuracy. A trusted AODV (TOAV) protocol was presented to mitigate routing attacks in MANET [34]. Herein trust value was represented by opinion. An acknowledgement based method namely 2ACK method was proposed to detect misbehavior in MANET environment [35]. This method was implemented on the top of dynamic source routing (DSR) protocol. In MANET, trust value of node was defined based on mobility, pause time, and remaining battery power [36]. However, consideration of inappropriate trust metrics is inefficient for providing security in MANET. Thus in majority of works, data security is not concentrated which increases vulnerability of data.

2.2. Survey on security mechanisms

AODV routing protocol was extended with level of trust (LOT) value [19]. Here LOT computation was performed by fuzzy approach. In fuzzy logic, trust value of node and throughput were taken as input and required encryption level was obtained as output. If an intermediate node has lower trust value and lower throughput then it requires high encryption. Then source encrypt the data and send the encrypted data to relay node. In this manner data security was achieved in this work. The transmitted data is subjected to alterations since data integrity is not ensured. In addition, packet dropping and packet redirecting attack are also held on the network. For securing group communication, three clustering algorithms were presented in MANET [20] as follows: (i) simple clustering algorithm, (ii) weighted clustering algorithm, and (iii) fuzzy clustering algorithm. In simple clustering algorithm, cluster formation is performed based on single metric known as connectivity. In weighted clustering algorithm, connectivity, energy, mobility, and distance were considered for cluster formation. In fuzzy based clustering, trust value of a node was computed in terms of number of successful transactions. Then in each cluster, group key was generated and distributed among CMs. However, CH selection by considering single metric (trust value) demands frequent CH selection in dynamic environment. Trust value computation based on number of successful transmissions is also not efficient.

To improve security against multiple threats, support vector machine (SVM) based intrusion detection system was proposed for ad-hoc networks [21]. In SVM classifier, average packet drop, average packet reception, and average packet interval were considered for attack detection. However, SVM is a supervised machine learning algorithm which requires huge data size and large time for training. In IoT environment, privacy and security was ensured by incorporating message authentication code (MAC) [22]. For that, a privacy-preserving communication protocol was designed with MAC. However, computing hash function for whole data increases computational complexity as well as memory consumption. In addition, this method is only able to provide data integrity and data security is not provided. In IoT environment, security was ensured by robust ECC based authentication protocol [23]. In this approach, each sensor was registered and authenticated through ECC protocol. Following security services were provided by this method: anonymity, untracebility, forward secrecy, and backward secrecy. Perhaps, this protocol provides authenticity; this method is not able to ensure data security and integrity. In IoT network, communication between nodes and server was secured by heterogeneous ring signcryption scheme [24]. The major objective of this scheme was to defend against ciphertext attacks in the network. This scheme increases time consumption with increase in number of nodes.

Thus all previous research works consider trust value for attack detection in ad-hoc network. However, the trust computation is also vulnerable since malicious node can modify this trust value. Similarly, none of these works is able to achieve data security and data integrity jointly without increase in computational complexity.

3. Problem Definition

In this section, we exploit major problems identified in MANET and IoT for security provisioning. Trusted security AODV (TS-AODV) protocol was designed with IDS to mitigate flooding attack, Blackhole attack, and Grayhole attack [25]. In IDS, a source-trust-rate was provided based on number of route requests generated. Here trust value for source node was computed as follows,

$$Source - Trust = (RREQ\ Count)^{-1} \qquad (1)$$

In eqn.(1), trust value for source node was computed based on number of RREQ packets forwarded by that node. However, trust value computation is ineffective since in AODV, each intermediate node broadcast RREQ packet for route selection. Furthermore, route selection based on trust value alone increases number of retransmissions due to frequent link breakages. Fuzzy logic based trust management mechanism were proposed in MANET [26], [27]. In fuzzy based OLSR routing, packet delivery ratio (PDR), and delay were considered for trust computation. However, both PDR and delay metrics are not only affected by malicious activities but also affected by other factors. Thus trust computation based on PDR and delay is not effectual. Fuzzy based secure architecture (FBSA) was comprised with training and testing phases. Based on fuzzy rules, the network nodes were categorized into malicious, normal, and best node. Here malicious activity is identified by fuzzy rules in which involvement of training phase increases time consumption. In addition, this method is able to identify malicious activities only; not able to detect malicious activities exactly. For mitigating Blackhole attack, a secure-AODV (SAODV) protocol was designed [28]. In SAODV, the first RREP packet received by source node was dropped and the node which sends RREP packet was considered as Blackhole attacker. Nonetheless, it is not ensured that first RREP packet is always malicious. Thus dropping first RREP request is not an intelligent wayto mitigate malicious attack. In addition, SAODV detects only affected path instead of detecting Blackhole attacker.

The problems highlighted in this section are considered in our work and resolved by our novel approaches. The major problems identified in this section are: (i) trust management is not accurate, (ii) route selection is not effectual, and (iii) attack detection is not efficient. Furthermore, data security and integrity is not ensured in all above works.

4. Proposed Secure MANET-IoT

4.1. Network Overview

To improve security and integrity, we design a novel group based routing scheme and flawless trust formulation for MANET-IoT environment. The overall proposed network environment is illustrated in figure.2. Our network environment comprises following entities: n number of MANET-IoT devices/nodes as $N = N_1, N_2, .., N_n$, certificate authority (CA), k number of security monitors $SM = \{SM_1, SM_2, \dots, SM_k\}$, and malicious devices. Security monitors are responsible for malicious node detection, recommendation filtering and secure group formation. Initially, the devices are grouped by security monitors after certificate verification. For flawless trust value formulation, security monitors utilize RF-K means algorithm. Further, route selection is involved with hybrid optimization algorithm which is effectively designed by combining GA and FFA algorithm with new fitness formulation. Data security and integrity are assured by HMAC-AES algorithm during data transmission. Each significant process is explained in following subsections.

4.2. Secure Group Formation

Integration of MANET and IoT to design MANET-IoT supports many applications and has many advantages. However, mobility management in MANET-IoT becomes challenging issue since the network topology is dynamically changed due to dynamic mobility of devices. In order to manage this kind of dynamic environment, grouping is an effectual solution. Thus we perform grouping of IoT devices by using SCGF algorithm.

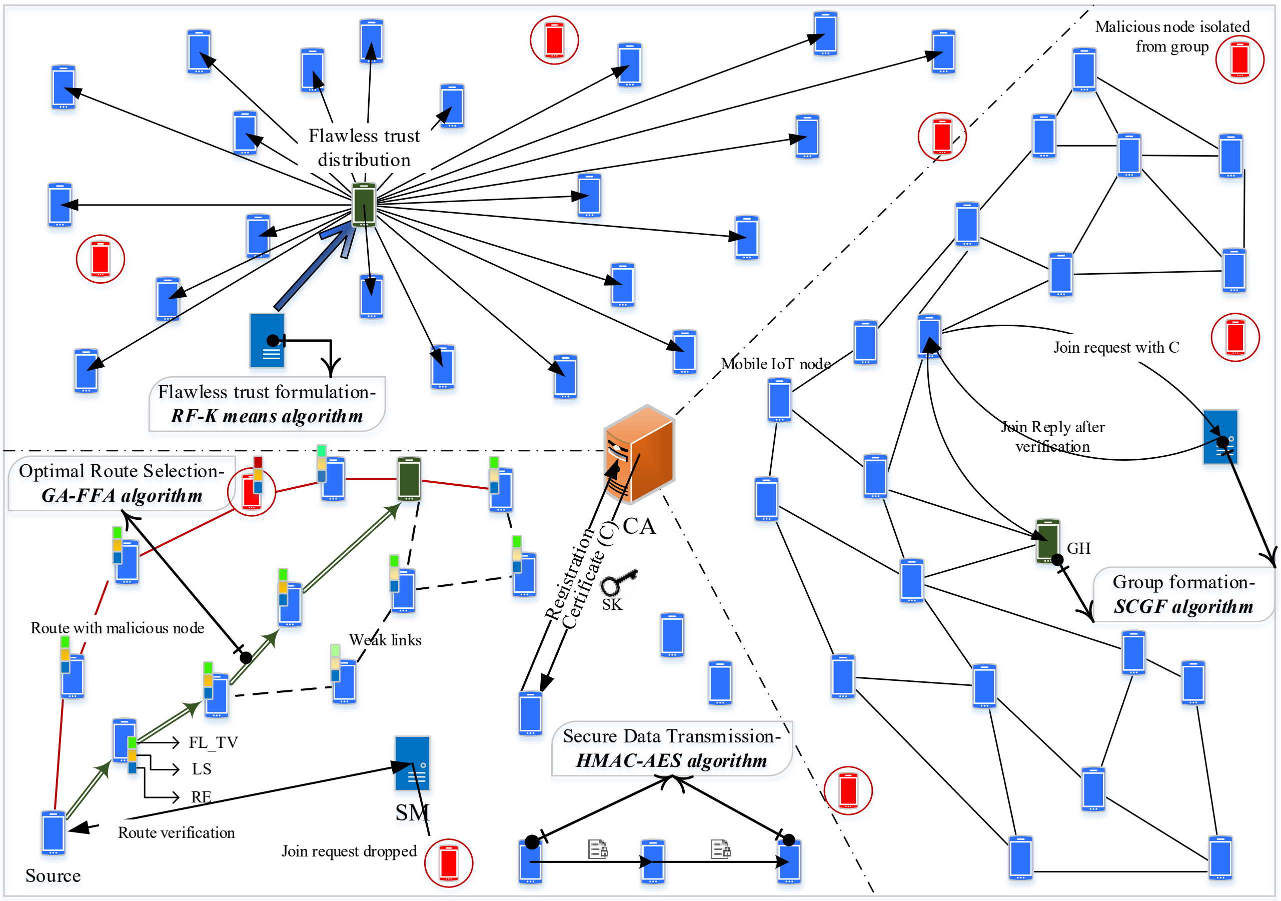


Figure 2. Proposed Secure MANET-IoT environment

Involvement of SCGF algorithm improves network management as well as security of the network through certificate verification. Initially, the network is divided into regions based on security monitors. The nodes within the range of each SM belong to corresponding group that is formed by that SM. SCGF algorithm is initiated with optimal GH selection. For optimal GH selection, weighting factor (WF) is formulated as follows,

$$WF(N_i) = E_{N_i} - (M_{N_i} + AD_{N_i}) \qquad (2)$$

The weighting factor of 'i^{th}' node N_i is computed based on energy level (E_{N_i}), mobility (M_{N_i}), and average distance with neighbor nodes (AD_{N_i}). A node with highest WF in particular region is selected as GH by SM. Then the selected GH is verified through certificate verification. For this purpose, all IoT nodes must be registered with CA in order to obtain certificate (C) and secret key (SK) to form secure group. Each node submits its unique ID (ID) and password (PW) to CA during registration. Then the CA provides a digital certificate to that corresponding node. The digital certificate consists of ID of the node, signature of CA ($Sign(CA)$), and secret key of node, and unique certificate ID ($ID(C)$). After the completion of registration, CA distributes the certificates of registered nodes to SMs for further verification. The selected GH submits its $\{ID\|C\}$ to SM in order to receive group secret (GS). When GH submits the $\{ID\|C\}$, SM verifies whether the node is legitimate or not. For verification, SM checks the $Sign(CA)$ in C and encrypt the GS by using secret key of GH. If the node is legitimate SM sneds GS to that node in encrypted form ($En\{GS\}$) and broadcast the GH selection message to all other nodes in that region. Thus the node must decrypt the GS in order to join with group. Upon receiving, GH selection message, all other nodes sends $JoinReq$ to GH. However, for group formation the node must have GS obtained from SM (i.e.) the node must be verified by SM. If GS submitted by node is matched with GS provided by SM, then GH sends $JoinRep$ to that node. Otherwise, GH deny the access of that node from group formation. Thus in SCGF algorithm, the legitimate nodes in the region form secure group to establish communication among nodes. Here malicious nodes are isolated form the group through verification.

In figure.3, the process of SCGF algorithm is illustrated. Thus involvement of SCGF algorithm isolates malicious and non-legitimate nodes in each region through secure group formation. Secure group formation supports dynamic network management and also supports flawless trust formulation through recommendation filtering.

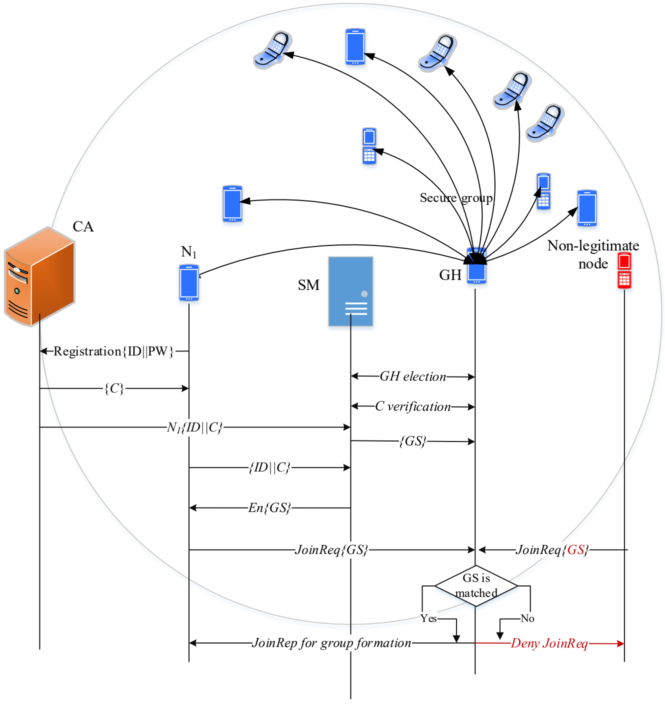


Figure 3. SCGF algorithm based group formation

4.3. Flawless Trust Formulation

In MANET-IoT network, majority of attackers are identified by analyzing trust value. Thus trust value computation plays vital role in security provisioning in MANET-IoT. However, trust value is also subjected to security threats such as trust value distortion attacks. In this type of security threats, the malicious nodes alter the trust value of other nodes during indirect trust computation which introduces unnecessary conflicts in the network. In addition, inaccurate trust computation leads to ineffectual attack detection. In our work, we adapt RF-K means algorithm for flawless trust formulation as well as for Grayhole attack detection. RF-K means algorithm is performed by SM for trust computation. For each node, SM computes flawless trust value (FL_TV) based on trust value provided by other nodes. Thus for each node FL_TV, SM performs RF-K means algorithm. The process of RF-K means algorithm in flawless trust formulation and Grayhole attack detection is described in following steps,

Step 1: In this step, SM collects TV from all nodes in the region through GH. In our work, each node computes TV for its neighboring nodes and transmits it to corresponding GH periodically. Then GH aggregates the TV and sends TV to SM. The TV that is transmitted to SM is in the form of $[N_1 \rightarrow \{TVs\}, N_2 \rightarrow \{TVs\}, .., N_j \rightarrow \{TVs\}]$ (i.e.) the node ID (N_1) and its corresponding trust values are provided by other nodes (TVs). Each node computes TV of neighboring nodes as follows,

$$TV = \frac{TR}{BS+DR} \tag{3}$$

For a node TV is computed in terms of transmission rate (TR), buffer size (BS), and drop rate (DR). Transmission rate of a node (TR) is computed as follows,

$$TR = \frac{Number\ of\ packets\ forwarded}{Total\ NUmber\ of\ packets\ sent} \tag{4}$$

Similarly BS and DR can be calculated as follows,

$$BS = \frac{Buffer\ Utilized}{Buffer\ Size} \tag{5}$$

$$DR = \frac{Number\ of\ packets\ dropped}{Total\ number\ of\ packets\ sent} \tag{6}$$

Step 2: In this step, SM performs RF-K means algorithm for each node based on TVs provided by other neighboring nodes. For this purpose, SM initializes number of clusters Kvalue. Thus for each node, K number of clusters are formed for TVs.

Step 3: Randomly initialize number of centroid as follows,

$$Centroids = \{TV_{C1}, TV_{C2}, \dots, TV_{CK}\} \tag{7}$$

Here the centroids initialized are trust values of a node. Let N_1 has TVs as $TV = \{TV_1, TV_2, .., TV_L\}$. Thus from this set of TVs, K number of centroids are initialized in random manner.

Step 4: Assign TVs to nearest centroid based on trust distance ($Tdis$) value. Here the $Tdis$ is computed as the difference between TV and centroid. For 'k^{th}' TV, the difference with 'j^{th}' centroid is computed as,

$$Tdis = |TV_{Cj} - TV_k| \tag{8}$$

$$If\ Tdis(j,k) = Small, \quad assign\ TV_K \rightarrow TV_{Cj} \tag{9}$$

Eqn.(9) represents that the TV_k is assigned to centroid which minimizes $Tdis$. In this manner, all TVs are assigned to closest centroid.

Step 5: In this step, all centroids are updated (i.e.) recomputed. Then all above steps are performed with new centroid until optimal 'K' clusters are formed. In this step 'K' number of recommendation clusters ($RCls$) are formed as,

$$RCls = \{RCls_1, RCls_2, \dots, RCls_K\} \tag{10}$$

Step 6: In this step, weighted inter-cluster difference is computed in order to exploit Grayhole attack detection. Typically Grayhole attacker is a selective forwarding attacker which forwards data from selective sources and drops data from other nodes. In this case, trust value which is computed by particular node is too large while by other nodes are low for an attacker. Thus there is high possibility to the attacker to be considered as honest node. In order to avoid this conflict, RF-K means algorithm performs inter-cluster distance computation. Before that, each TV in each cluster is weighted based on following function,

$$W(TV_j) = \frac{\sum_{i=1}^{X} \Delta(TV_j, TV_i)}{X} \tag{11}$$

$$Weighted\ TV_j = TV_j \times W(TV_j) \tag{12}$$

Here X represents number of TVs in the cluster and $\Delta(TV_j, TV_i)$ represents difference with 'i^{th}' TV. In this manner, each trust value is computed as $weighted\ TV$ in this step. After completion of $weighted\ TV$ computation, average $weighted\ TV$ is computed for each cluster as follows,

$$AvgTV = \frac{\sum_{j=1}^{X} Weighted\ TV_j}{X} \tag{13}$$

This average TV is computed for each cluster in $RCls$. Then inter-cluster cluster distance is computed as follows,

$$ICd = |RCl_1 - RCl_2| \tag{14}$$

Eqn.(14), represents the inter-cluster distance (ICd) between two clusters RCl_1 and RCl_2. If this distance is small, then the node is not a Grayhole attacker. Otherwise the node is considered as Grayhole attacker since Grayhole attacker obtains high TV from particular nodes and obtains low TV from other nodes.

Step 7: In this step, flawless TV computation is performed based on majority rule. For each FL_TV is computed as $AvgTV$ of cluster with large number of TVs (i.e.) the TV which is provided by majority of nodes is assigned as FL_TV as follows,

$$FL\_TV(j) = AvgTV(j), if\ X = larger \tag{15}$$

Thus in RF-K means algorithm, Grayhole attacker is detected effectually and also FL_TV computation is accomplished. The computed FL_TV for each node is distributed to all other nodes in the group through GH. Then this TV is further used for optimal route selection.

Pseudocode for RF-K means

```
Input: $K$, collected $TVs$ for all nodes
Output: $Grayhole\ attack\ detection$, $FL\_TV$ formulation
    Begin
For $N_i \in group$
    Collect $TV = \{TV_1, TV_2, .., TV_L\}$from $GH$
    Initialize centroids
    For each $TV_J \in TV$
        Compute $Tdis$ with centroids
        Assign $TV_j$ to centroid which $minimize\ Tdis$
    End for
    Update centroids
    Form $RCls = \{RCls_1, RCls_2, \dots, RCls_K\}$
    For each $TV \in RCl$
        Compute $W(TV)$ using(11)
        Find $Weighted\ TV$ using (12)
    End for
    For all $RCls$
        Compute $AvgTV$
        Find $ICd$
          If $ICd == Low$
            $N_i is\ a\ Grayhole\ attacker$
          Else
            $N_i is\ honest$
          End if
          Compute $FL\_TV$ using (15)
      End for
End for
End
```

The above pseudocode explains the procedure of proposed RF-K means algorithm. This algorithm can be explained through an example. Consider a node N_i has three neighbour nodes as N_{i+1}, N_{i-1}, and N_{i+2}. Each node provides TVs for N_i as follows, $N_{i+1} \rightarrow 10, N_{i-1} \rightarrow 11, N_{i+2} \rightarrow 2$. In this case, two $RCls$ are formed as $RCl_1 = \{10,11\}$ and $Rcl_2 = \{2\}$. The $Weighted\ TV$ in each cluster is computed as $RCl_1 = \{5.25\}$, and $RCl = \{2\}$. Thus $ICd = 3.25$. Here inter-cluster distance is high, thus the node is considered to be an attacker (i.e.) N_i forwards legitimately from N_{i+2} and drops packets from other nodes. In this manner, Grayhole attack detection is carried out by RF-K means algorithm.

4.4. Hybrid optimization algorithm for secure routing

In this section, we propose a hybrid optimization algorithm for secure route selection for data transmission. Involvement of adversaries in the network increases the packet loss in the network. To secure data transmission, it is necessary to select trusted path between source and destination. However, MANET-IoT is highly dynamic which also requires optimal route for data transmission. Thus we propose GA-FFA algorithm for optimal route selection between source and destination. GA is a well-known algorithm that has been employed for optimal route selection in MANET [29]. Although GA provides optimum route for data transmission, it consumes large time for convergence. On the other hand, FFA algorithm shows efficiency in route optimization for MANT [30]. In order to mitigate the issue of GA, a new FFA algorithm is integrated with GA for route selection. In GA-FFA algorithm, multiple available paths between source (Src) and destination (Des) are generated by GA and an optimal route is selected by FFA algorithm. In GA algorithm, the available paths are generated by applying $crossover$ and $mutation$ operators. Then these available paths are initialized as fireflies in FFA algorithm. In all available paths, route request (RREQ) is sent by Src and route reply ($RREP$) is sent by intermediate nodes. In order to detect Blackhole attacker, the sequence number ($SeqNum$) of all RREP packets is analyzed. If $SeqNum$ difference is large, then the node which sent RREP packet s considered as malicious node. Then this route is eliminated from available paths. After elimination of attacker path, finally the following multiple paths are initialized in FFA algorithm,

$$AP = \{R_1, R_2, .., R_Y\} \qquad (16)$$

In GA, Y number of routes are generated between Src and Des. Then all available paths (AP) are initialized in FFA algorithm.

In FFA algorithm following rules are deployed for optimal route selection,

- All fireflies are unisex (i.e.) attracts each other regardless of their gender
- Attractiveness is directly proportional to brightness and distance is inversely proportional to both attractiveness and brightness
- Objective function is used to determine the brightness level.

Based on above rules, the process of FFA for optimal route selection is performed as follows,

1. Formulation of objective function (OF) as follows,

$$OF = Max(\frac{FL\_TV, RE, LS}{HC}) \qquad (17)$$

The objective function of our proposed GA-FFA algorithm is to select optimal route that maximizes FL_TV, RE, link stability (LS), and minimizes hopcount (HC).

2. Initialize all available routes $AP = \{R_1, R_2, .., R_Y\}$ fireflies in the population.
3. Computation of light intensity ($I(R)$) is performed based on OF as follows,

$$I \propto OF(R) \qquad (18)$$

4. Attractiveness between two fireflies is formulated as follows,

$$\beta = \beta_0 e^{-\gamma r^2} \qquad (19)$$

The attractiveness is determined based on light absorption coefficient (γ), and attractiveness at $r = 0$ (β_0), and the distance between those fireflies (r).

5. Movement of firefly towards more attractive firefly (i.e.) optimal solution is determined as,

$$x_i = x_i + \beta_0 e^{-\gamma r}(x_j - x_i) + \alpha\varepsilon \qquad (20)$$

6. Update light intensity based on movement and rank the fireflies accordance with light intensity.
7. Select optimal route (OR) over iteration
8. End the process

By executing all above steps, the GA-FFA algorithm selects optimal route (OR) between Src and Des. In GA-FFA algorithm OF is formulated based on significant routing metrics which improves security as well as efficiency of data transmission. Selection of optimal route based on FL_TV minimizes the possibility of adversaries in the particular route. Thus proposed GA-FFA algorithm ensures high level security as well as data transmission efficiency in MANET-IoT network.

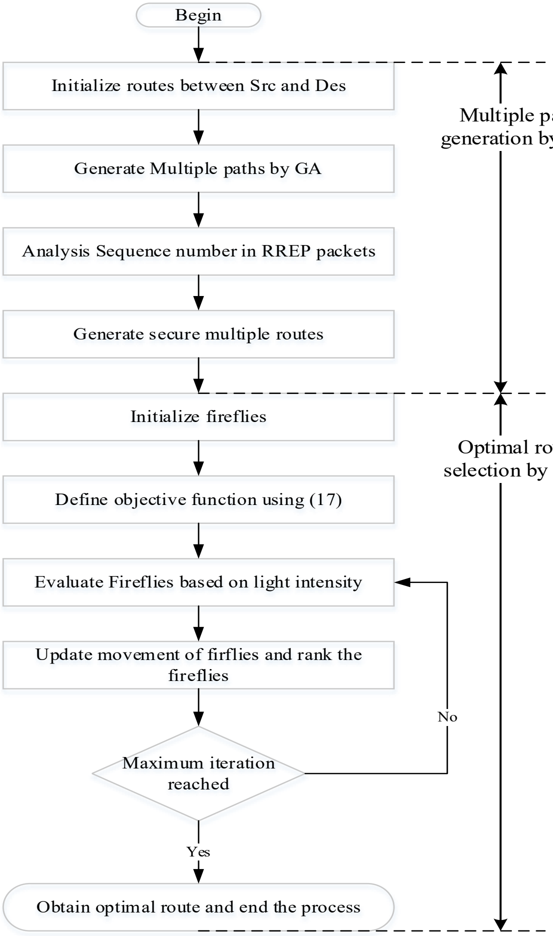

Begin
Initialize routes between Src and Des
Generate Multiple paths by GA
Analysis Sequence number in RREP packets
Generate secure multiple routes
Initialize fireflies
Define objective function using (17)
Evaluate Fireflies based on light intensity
Update movement of firflies and rank the fireflies
Maximum iteration reached
No
Yes
Obtain optimal route and end the process
Multiple path generation by GA
Optimal route selection by FFA

Figure 4. Process of GA-FFA algorithm

In figure.4, the entire process involved in GA-FFA algorithm is illustrated. Here GA algorithm generates multiple available paths and the affected paths are eliminated by sequence number analysis. Then the secure routes which are free from Blackhole attack are initialized in FFA algorithm to identify optimal route between Src and Des.

4.5. Data security and integrity provisioning

Perhaps, our proposed network is secured through secure clustering and routing; data security and integrity are still required for transmitted data to improve security level. To achieve data security and integrity jointly, we proposed a novel method that integrates hash function and cryptography function without increase in overhead and time consumption. For ensuring data security and data integrity, HMAC-AES algorithm is proposed. In HMAC-AES algorithm, the data (D) to be transmitted is divided into two equal blocks as $\{D_1, D_2\}$. Then the first block of the data (D_1) is encrypted by AES algorithm and the second data block (D_2) is involved with has generation by HMAC algorithm. AES algorithm involves four major transformations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey. Here encryption of data is performed through key expansion processes and each round key is stored in 4-byte words denoted as $w[z]$ In AES algorithm data encryption is performed as follows,

Pseudocode for AES encryption

```
Input: $SK$, $D_1$
Output: Ciphertext of $D_1$ $(En\{D_1\})$
Begin
Assign $State = \mathcal{M}$
AddRoundKey($State, \&w[0]$)
For ($z = 1 \quad step\ 1\ to\ 9$)
SubBytes ($State$)
ShiftRows ($State$)
MixColumns ($State$)
AddRoundKey ($State, \&w[z * 4]$)
End for
SubBytes ($State$)
ShiftRows ($State$)
AddRoundKey ($State, \&w[40]$)
End obtain $En\{D_1\}$
```

The above pseudocode explains the process of AES algorithm in data encryption. Here the first part of the data is encrypted and corresponding ciphertext $(En\{D_1\})$ is obtained. Forming data block, message authentication code (MAC) is generated to ensure data integrity using HMAC algorithm. HMAC based MAC generation is performed as follows,

$$HMAC(SK, D_2\} = H((K' \oplus opad) \| H((K' \oplus ipad) \| m)) \tag{21}$$

The overall process of HMAC based MAC generation is performed illustrated in following pseudocode. Thus in HMAC-AES algorithm the first data block is encrypted by AES algorithm and foe second data block MAC is generated by HMAC algorithm. Then the data is transmitted to destination in the form of $(\{En\{D_2\}, MAC\{D_2\})$ (i.e.) ciphertext of D_1, MAC of D_2, and plaintext of D_2. In destination, the ciphertext is decrypted using AES algorithm and the MAC in received data is verified by generating MAC for D_2.

Pseudocode for HMAC based MAC generation

```
Input: $SK$, $D_2$
Output: MAC generated for $D_2$
Begin
If ($length(SK) > blocksize$)
    $Key \leftarrow hash(SK)$
Else
    $Key \leftarrow Pad(SK, blocksize)$
End if
$o\_key\_pad = Key\ XOR\ [0 \times 5c * blocksize]$
$i\_key\_pad = Key\ XOR\ [0 \times 36 * blocksize]$
Obtain $MAC = H(o\_ke\_pad \| H(i\_key\_pad \| D_2))$
End
```

Thus AES algorithm provides data security whereas HMAC algorithm ensures data integrity. If any attacker obtains the data, the attacker is not able to obtain entire data without secret key. Similarly, the alterations made by attacker can be determined by HMAC algorithm. Thus our proposed work ensures both data security and data integrity for transmitted data.

5. Experimental Results and Simulation

In this section, we evaluate our proposed work with previous research works through necessary simulations. In this section, simulation environment of proposed secure MANET-IoT is briefly described and the comparative analysis is performed to measure the efficiency of our proposed work.

5.1. Simulation environment of MANET-IoT

Our proposed secure MANET-IoT that integrates MANET in IoT environment is simulated in network simulator-3.26 (ns-3.26) which is a discrete event simulator that supports various communication standards, and different networks. Our network comprises MANET-IoT devices, CA, SMs, and malicious nodes.

Table 1. Simulation parameters

Parameter	Value
Simulation area	1000×1000 m
Number of IoT devices	50
Number of CA	1
Number of SMs	5
Number of groups	5
Communication range of IoT device	100m
Mobility model	Random Way Point
Mobility speed	10 m/s

Total number of packets		100
Packet size		1000 bytes (Max)
Packet interval		1 s
Initial energy level		100 Joules
Number of retransmissions		7
Data rate		1 Mbps
GA-FFA	Initial population	100
	Crossover rate	0.7
	Mutation rate	0.001
	γ, β_0	1.0, 0.2
	Number of iteration	50
Simulation time		35s

In table.1, all significant simulation parameters considered in secure MANET-IoT implementation is illustrated. These parameters are not limited and all other parameters that support MANET-IoT are also considered in our work.

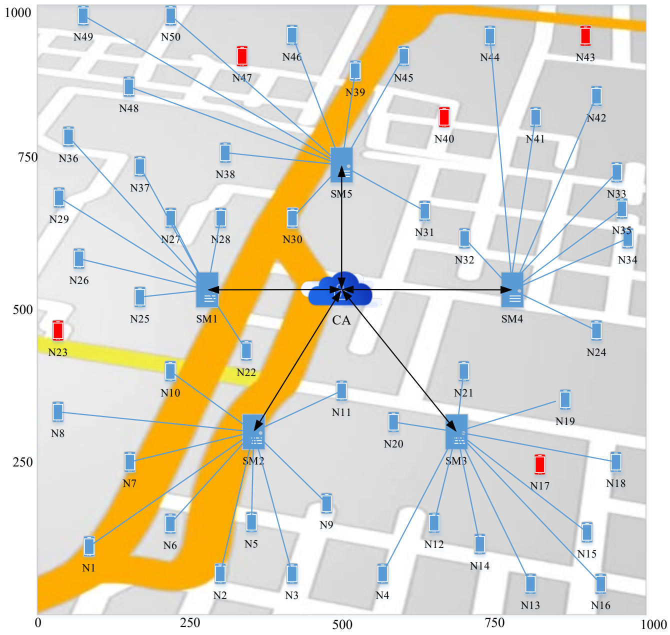


Figure 5. Simulation environment of MANET-IoT

In figure.5, the simulation environment of our proposed MANET-IoT is illustrated for smart city applications. Here the devices include mobile devices of humans, smart devices deployed on animals, vehicles and so on to perform specific operations. Our network environment comprises MANET-IoT devices which move around within the network area and malicious nodes which are looking for launching attack on communication between honest nodes. Here 5 nodes are malicious and those nodes are differentiated from honest nodes using red color. Based on SMs communication range, five groups are formed without malicious nodes.

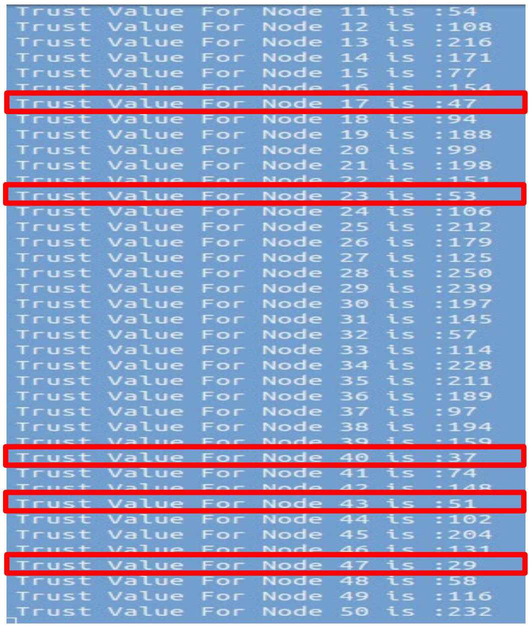
5.2. Obtained results in security provision

Our proposed work achieves data security and integrity by a novel HMAC-AES algorithm. In this sub-section, we provide security analysis of proposed work.

Table 2. Security analysis

Parameter	Value
Key size	128 bit
Number of rounds in AES	10
Block size	4
Average encryption time	4 ms
Average decryption time	5 ms
Number of malicious nodes	5 (10% of total nodes)
Attacks considered	Blackhole and Grayhole

In table.2, the security results obtained by our proposed work are depicted. In the network, each node is registered with CA and obtains unique certificate from CA. The FL_TV computed by RF-K means algorithm is depicted in figure.6. Here we can see that the malicious nodes such as $N17, N23, N40, N43, N47$ are given with lower trust values than other honest nodes. Involvement of flawless trust computation improves the trust value computation in our work.



```
Trust Value For Node 11 is :54
Trust Value For Node 12 is :108
Trust Value For Node 13 is :216
Trust Value For Node 14 is :171
Trust Value For Node 15 is :77
Trust Value For Node 16 is :154
Trust Value For Node 17 is :47
Trust Value For Node 18 is :94
Trust Value For Node 19 is :188
Trust Value For Node 20 is :99
Trust Value For Node 21 is :198
Trust Value For Node 22 is :151
Trust Value For Node 23 is :53
Trust Value For Node 24 is :106
Trust Value For Node 25 is :212
Trust Value For Node 26 is :179
Trust Value For Node 27 is :125
Trust Value For Node 28 is :250
Trust Value For Node 29 is :239
Trust Value For Node 30 is :197
Trust Value For Node 31 is :145
Trust Value For Node 32 is :57
Trust Value For Node 33 is :114
Trust Value For Node 34 is :228
Trust Value For Node 35 is :211
Trust Value For Node 36 is :189
Trust Value For Node 37 is :97
Trust Value For Node 38 is :194
Trust Value For Node 39 is :159
Trust Value For Node 40 is :37
Trust Value For Node 41 is :74
Trust Value For Node 42 is :148
Trust Value For Node 43 is :51
Trust Value For Node 44 is :102
Trust Value For Node 45 is :204
Trust Value For Node 46 is :131
Trust Value For Node 47 is :29
Trust Value For Node 48 is :58
Trust Value For Node 49 is :116
Trust Value For Node 50 is :232
```

Figure 6. Simulation environment of MANET-IoT

Then our proposed security algorithms such as SCGF algorithm, RF-K means algorithm, GA-FFA algorithm and HMAC-AES algorithm are performed in MANET-IoT in order to improve network security for various IoT applications.

5.3. Performance Evaluation and Comparative analysis

In this sub-section, we evaluate our proposed work in MANET-IoT network based on following performance metrics: packet delivery ratio (PDR), throughput, delay, and malicious activity detection. Our proposed work is compared with state-of-the-art works such as SOADV [28], FBSA [27], and conventional AODV. The performance metrics considered in our work are described as follows,

- ***PDR:*** PDR is defined as the ratio between number of packets transmitted by source node and the number of packets received by destination node successfully.
- ***Throughput:*** throughput is defined as the average rate of successful data transmission over a communication link in the network at given period of time.
- ***Delay:*** In the network, delay is defined as the average time taken by a data packet to reach the destination from source node.
- ***Malicious activity detection:*** This metric is defined as the ratio between number of malicious nodes identified by security scheme to the total number of malicious nodes in the network.
- ***Energy Consumption:*** In the network, energy consumption is estimated by computing energy consumed due to data transmission, data reception, and idle listening.

Table 3. Comparative Analysis

Parameter	AODV	SAODV	FBSA	Proposed
Routing algorithm	AODV	S-AODV	OLSR	GA-FFA
Route selection metrics	Distance	Distance	PDR & Delay	Flawless trust, residual energy, link stability, hop count
Security metrics	None	None	Trust	Flawless Trust
Data security	Not provided	Not provided	Not provided	Data is secured
Security algorithm	None	None	None	HMAC-AES
Trust mechanism	None	None	Based on PDR and delay	RF-K means

In table.3, comparative analysis between proposed work and state-of-the-art works has depicted. The analysis confirms that proposed work fulfills all security and routing requirements better than previous works.

Analysis on PDR

PDR is a significant metric that measures successful data transmissions held over the network. In the presence of malicious nodes, the packet loss is increased in the network which minimizes the PDDR.

In figure.7, we compare PDR obtained by proposed work with previous research works. Here we can see that, our proposed work achieves better PDR than previous works. When average speed of nodes is 2m/s, 96% of packets are transmitted to destination successfully in our work. In the same node speed, FBSA method transmits 94% of packets to destination and SAODV method transmits 36% of packets successfully to destination. Here SADOV method and AODV protocol are fail to provide better even upto 50%. In addition, FBSA method also provides PDR 2% lower than proposed work. This analysis shows that involvement of effectual security schemes and optimal routing in proposed work improves PDR of the network. The previous works are not able to achieve better PDR since the involvement of adversaries which limits the network performance.

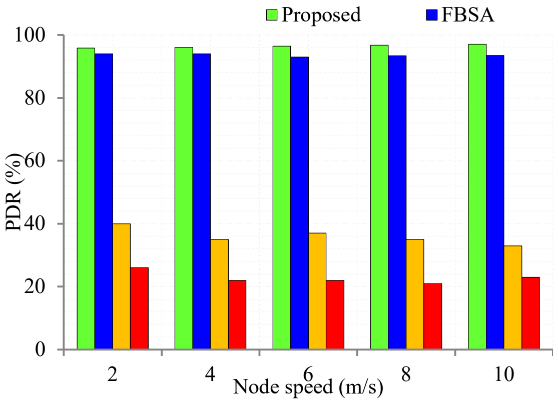


Figure 7. Comparative analysis on PDR

Analysis on throughput

Network throughput is an significant metric that measures the performance of entire network. In the presence of adversaries this metric is low (i.e.) in a secure environment throughput is large.

In figure.8, throughput metric achieved by our proposed work is compared with previous works. Our proposed work achieves throughput upto 140kbps even in high mobility (i.e.) 10m/s. perhaps, the modes are highly dynamic; selection optimal route by GA-FFA algorithm and group formation by SCGF algorithm improves the performance of the network. In addition, formulation of FL_TV helps in detection of highly secure route which further improve network performance. In FBSA method, the throughput is only 121kbps which is 20kbps lower than our proposed approach. Absence of secure routing and mobility management scheme results in lower throughput performance. But conventional AODV and AODV protocols are not able to handle large number of adversaries and high dynamic mobility. Thus both protocols are not able to improve network throughput.

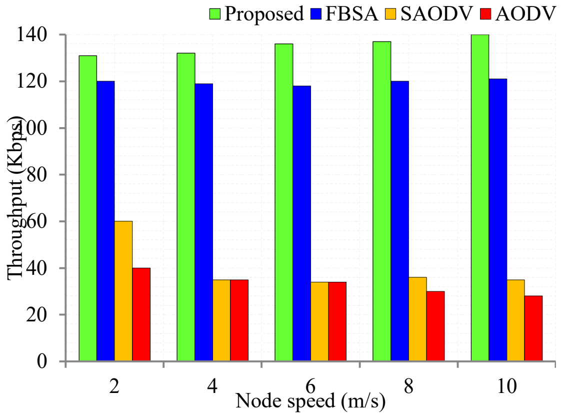


Figure 8. Comparative analysis on throughput

Analysis on delay

In mobile network environment, delay is significant since it is increased with increase in node mobility. Thus this analysis will show the ability of the work to cope with dynamic environment.

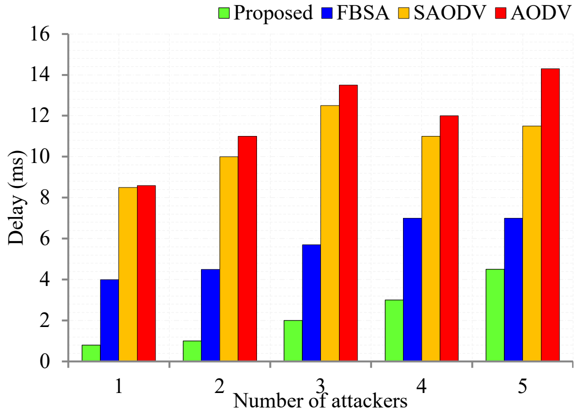


Figure 9. Comparative analysis on delay

In figure.9, proposed work is analyzed in terms of delay metric. The analysis shows that proposed work minimizes delay (i.e.) in our proposed work the data is transmitted to destination from source node within minimum transmission time. The delay is increased with increase in number of attackers. This is because; involvement of attackers disrupts data transmission through packet dropping, data redirection and so on. However, our proposed work improves delay even in the presence of five malicious nodes. The reason behind improved delay in our work is that involvement of FL_TV, secure grouping, and secure routing minimizes delay metric in the network. The previous methods results in large time delay which degrades the performance of the network. This analysis confirms that FBSA, SAODV methods are not able secure network environment. the results obtained for AODV protocol shows that absence of security scheme results in increased adversaries which not suitable for mobile environment. in the presence of five attackers, proposed work provides 4.5ms of delay which is relative lower than previous works.

Table 4. Efficiency of proposed work in data transmission

Method	PDR (%)	Throughput (kbps)	Delay (ms)
AODV	23	32	14
SAODV	36	40	13
FBSA	93	119	7.6
Proposed	96.3	135	3.26

In table.4, efficiency of our proposed work in data transmission is analyzed in terms of performance metrics. From the analysis we can conclude that proposed work achieves better performance in data transmission. Involvement of secure group formation supports mobility management while involvement of FL_TV formulation relaxes the problem of adversaries in data transmission. In addition, secure routing and secure data transmission protect the data from adversaries which increases number of retransmissions. Thus each significant process involved in our work contributes in efficient data transmission in MANET-IoT environment.

Analysis on malicious activity detection

The prime objective of our work is to minimize the presence of adversaries in the network. To analyze the security strength of our proposed work, we analyze malicious activity detection rate.

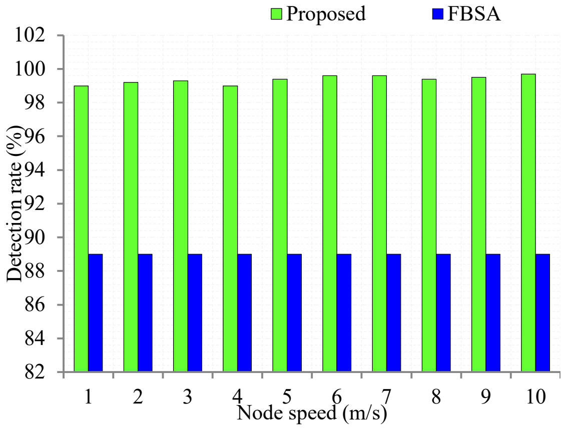


Figure 10. Comparative analysis on malicious activity detection

In figure.10, detection rate achieved by proposed work and previous FBSA method is compared. The graphical illustration shows that our proposed work is effectual in malicious activity detection. Averagely, our proposed work achieves 10% better detection rate than FBSA method. In our work, 99% of malicious nodes are identified accurately whereas in FBSA method only 89% of malicious nodes are detected correctly. Both methods utilize trust value for malicious activity detection. However, our proposed work improves detection rate with significant trust value computation by flawless trust formulation. In addition, secure route selection also minimizes involvement of adversaries in the network. Thus with the support of *FL_TV* formulation, our proposed work improves malicious activity detection rate upto 96%.

Table 5. Analysis on malicious node detection

Parameter	FBSA	Proposed
Number of nodes	50	50
Number of malicious node	5	5
Number of malicious nodes identified accurately	≅4	≅5
Detection rate	89%	99%

In table.5, the detection rate achieved by proposed work and FBSA method is analyzed. In our work, 99% of malicious nodes are detected accurately (i.e.) all 5 malicious nodes are identified accurately. But in FBSA method, 4 nodes only detected as malicious nodes. Thus our proposed work is efficient in attack detection rate.

Analysis on energy consumption

In literature, security provisioning approaches often increases energy consumption. In this subsection, energy consumption is analyzed with respect to malicious activities.

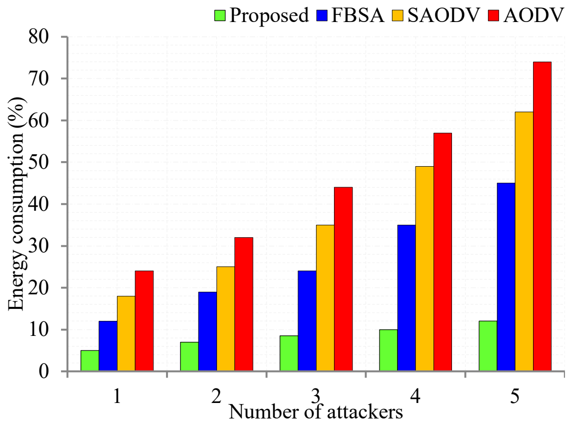


Figure 11. Comparative analysis on energy consumption

In figure.11, energy consumption is analyzed based on number of attacker nodes in the network. In the graph, we can see that proposed work consumes only 12% of energy even with 5 attackers. However, for the same number of attackers FBSA scheme consumes nearly 45% of energy due to absence of effectual security scheme. Likewise, SAODV and AODV consume 62% and 74% of energy respectively. The major reason for this huge energy difference is, previous approaches require large number of retransmissions due to involvement of malicious nodes. But in proposed work, malicious nodes are identified accurately and optimum path is selected for route election. Thus combined security provision and optimal route selection minimizes energy consumption in the network.

Table 6. Analysis on energy consumption

Method	Initial energy (J)	Average Energy consumption (%)
AODV	100	46.2
SAODV	100	37.8
FBSA	100	27
Proposed	100	8.5

In table.6, average energy consumption metric is compared with for each work. The analysis shows that proposed work achieves relatively minimum energy consumption (8.5%) which is 17% lower than FBSA method, 29% lower than SAODV, and 37% lower than conventional AODV scheme.

6. Conclusion

In this paper, a novel security scheme is proposed with flawless trust formulation mechanism for MANET-IoT environment. To improve network management, the network is initially grouped by SCGF algorithm in secure manner. In each secure group, flawless trust computation is performed by SM using RF-K means algorithm. Flawless trust computation uses recommendation filtering approach which also helps in Grayhole attack detection. For secure as well as effectual data transmission, GA-FFA based optimal route selection algorithm is presented. Here GA-FFA algorithm utilizes a new fitness value that is formulated by flawless trust value and significant routing metrics. The transmitted data is secured by HMAC-AES algorithm that combines cryptography function and hash function together. HMAC-AES algorithm also assures data integrity which is significant for mobile environment. Experimental results show that proposed work is effectual in PDR, throughput, delay, malicious activity detection, and energy efficiency. From the achieved results, it is clear that proposed work better in network management as well as security. On the whole, our proposed work achieves data security and integrity with improved data transmission in MANET-IoT environment. In future, we have planned to extend this work with energy efficient schemes. Although the results have shown that proposed work achieves better energy efficiency we aim to improve further energy efficiency of the network without loss in security level.

References

[1] Leite, J.R., Ursini, E.L., & Martins, P.S. (2017). Simulation of AdHoc Networks Including Clustering and Mobility. ADHOC-NOW.

[2] Anjum, S.S., Noor, R.M., & Anisi, M.H. (2017). Review on MANET Based Communication for Search and Rescue Operations. Wireless Personal Communications, 94, 31-52.

[3] Kandari, S., & Pandey, M.K. (2016). Impact of Residual Life Estimator Battery Model on QoS Issues in MANET. Wireless Personal Communications, 86, 601-614.

[4] Giri, A., Dutta, S., Neogy, S., Dahal, K., & Pervez, Z. (2017). Internet of Things (IoT): A Survey on Architecture, Enabling Technologies, Applications and Challenges. International Conference on Internet of Things and Machine Learning.

[5] Razzaque, M.A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2016). Middleware for Internet of Things: A Survey. IEEE Internet of Things Journal, 3, 70-95.

[6] Jabbar, W.A., Saad, W.K., & Ismail, M. (2018). MEQSA-OLSRv2: A Multicriteria-Based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT. IEEE Access, 6, 76546-76572.

[7] Bujari, A., Furini, M., Mandreoli, F., Martoglia, R., Montangero, M., & Ronzani, D. (2018). Standards, Security and Business Models: Key Challenges for the IoT Scenario. Mobile Networks and Applications, 23, 147-154.

[8] Liu, G., Yan, Z., & Pedrycz, W. (2018). Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey. J. Network and Computer Applications, 105, 105-122.

[9] Gurung, S., & Chauhan, S. (2018). A novel approach for mitigating gray hole attack in MANET. Wireless Networks, 24, 565-579.

[10] Gupta, P., Goel, P., Varshney, P., & Tyagi, N. (2019). Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET.

[11] Dorri, A. (2017). An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. Wireless Networks, 23, 1767-1778.

[12] Airehrour, D., Gutiérrez, J.A., & Ray, S.K. (2016). Securing RPL routing protocol from blackhole attacks using a trust-based mechanism. 2016 26th International Telecommunication Networks and Applications Conference (ITNAC), 115-120.

[13] Ahmed, M.N., Abdullah, A.H., Chizari, H., & Kaiwartya, O. (2017). F3TM: flooding factor based trust management framework for secure data transmission in MANETs.

[14] Kushwaha, A., Sharma, H.R., & Ambhaikar, A. (2016). A Novel Selective Encryption Method for Securing Text Over Mobile Ad Hoc Network.

[15] Jain, A., Tokekar, V., & Shrivastava, S.K. (2018). Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks.

[16] Panos, C., Ntantogian, C., Malliaros, S., & Xenakis, C. (2017). Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. Computer Networks, 113, 94-110.

[17] Singh, O., Singh, J., & Singh, R. (2017). Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET. Cluster Computing, 1-13.

[18] Schweitzer, N., Stulman, A., Margalit, R.D., & Shabtai, A. (2017). Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks. IEEE Transactions on Mobile Computing, 16, 2174-2183.

[19] Garg, M.K., Singh, N., & Verma, P. (2018). Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs. Elsevier, 132, 653-658.

[20] Gomathi, K., Parvathavarthini, B., & Saravanakumar, C. (2017). An Efficient Secure Group Communication in MANET Using Fuzzy Trust Based Clustering and Hierarchical Distributed Group Key Management. Wireless Personal Communications, 94, 2149-2162.

[21] Shams, E.A., & Rizaner, A. (2018). A novel support vector machine based intrusion detection system for mobile ad hoc networks. Wireless Networks, 24, 1821-1829.

[22] Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2016). A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. IEEE Internet of Things Journal, 4, 1844-1852.

[23] Li, X., Niu, J., Bhuiyan, M.Z., Wu, F., Karuppiah, M., & Kumari, S. (2018). A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 14, 3599-3609.

[24] Li, F., Zheng, Z., & Jin, C. (2016). Secure and efficient data transmission in the Internet of Things. Telecommunication Systems, 62, 111-122.

[25] Kumar, V.V., & Ramamoorthy, S.K. (2018). Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET. International Conference on Computing and Communications Systems, Springer, pp. 49-63.

[26] Tan, S., Li, X., & Dong, Q. (2016). A Trust Management System for Securing Data Plane of Ad-Hoc Networks. IEEE Transactions on Vehicular Technology, 65, 7579-7592.

[27] Bisen, D., & Sharma, S. (2018). Fuzzy Based Detection of Malicious Activity for Security Assessment of MANET. National Academy Science Letters, 41, 23-28.

[28] Jain, A.K., & Tokekar, V. (2015). Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks. 2015 International Conference on Pervasive Computing (ICPC), 1-6.

[29] Yen, Y., Chan, Y., Chao, H., & Park, J.H. (2008). A genetic algorithm for energy-efficient based multicast routing on MANETs.

[30] Persis, D.J., & Robert, T.P. (2016). Reliable Mobile Ad-Hoc Network Routing Using Firefly Algorithm.

[31] Sumra, I.A., Sellappan, P., Abdullah, A.V., & Ali, A. (2018). Security issues and Challenges in MANET-VANET-FANET: A Survey. EAI Endorsed Transactions on Energy Web and Information Technologies, 5 (17).

[32] Wang, P., & Zhang, P. (2016). A Review on Trust Evaluation for Internet of Things. MobiMedia.

[33] Kumar, A., Vishnoi, P., & ShimiS., L. (2019). Smart Grid Security with Cryptographic Chip Integration. EAI Endorsed Trans. Energy Web, 6, e6.

[34] Li, X., Lyu, M.R., & Liu, J. (2004). A trust model based routing protocol for secure ad hoc networks. 2004 IEEE

Aerospace Conference Proceedings (IEEE Cat. No.04TH8720), 2, 1286-1295 Vol.2.

[35] Liu, K., 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.