Received: March 22, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Soft-Computing Based Trust Management Framework for Group Key Management in MANETs

Nagaraja Gundluru[1*] **Pradeep Reddy Ch[1]**

[1]*School of Information Technology & Engineering, VIT University, Vellore, India*
* Corresponding author's Email: nagaraja.g@vit.ac.in

Abstract: We can realize instant joint group communication by forming Mobile Ad Hoc Networks without demanding any pre-plan or pre-existing infrastructure setup. Conversely, the curbs of these networks such as unreliable wireless medium, unpredictable topology, no central administration, fuel the compulsion of a key based cryptographic algorithm to defend data traffic. In this perspective, substantial research work has been done in the last decade or so and ascertained that the trust based frameworks for group key management deliver superior performance than others. Since the nodes in ad hoc networks have limited computing resources, the overall performance of the system depends on how effectively and securely designed the system. This encourages us to work on a framework which consumes less computing power and also invulnerable to internal as well as external attacks. We propose a framework which reduces the network resource consumption for the trust request and collection using game theory concept. The energy of the wireless nodes are significantly saved by choosing the novel strategy called as finding optimal set of remote nodes to send the response for trust request using game theory. Choosing local optimal at each stage eventually leads to global optimal. Later, synthesize the collected trust and handle the attacks using fuzzy concept in order to get the degree of trustworthiness instead of binary classification. We prove with our simulation results that our proposed scheme reduces overhead of the network significantly while without compromising security aspects.

Keywords: Mobile ad hoc network, Group key management, Game theory, Fuzzy logic, Trust management framework, Attacks, Dishonest nodes.

1. Introduction

1.1 Mobile ad hoc networks

A mobile ad hoc network (or MANET) is a wireless network comprises of mobile nodes which need petty or infrastructure-less to deploy instantly and facilitate group communication. It has a dynamic topology due to a node may join in, leave from, or move around the network at any point of time [1]. Since a MANET can be rapidly and suddenly organized, it has strengthened attractiveness in cooperative application situations such as disaster rescue operations, battlefields, conferences, etc. The majority of these setups assume there would be an efficient and secure group communication framework [2]. The hurdles to build such framework in MANETs comprise constrained computing power (i.e. Bandwidth, Battery, CPU, Memory, etc.) of each wireless node, untrustworthy wireless medium and irregularity in network topology due to node mobility. In a MANET, there is a direct communication between neighbors within the range of wireless medium; otherwise, via intermediate nodes if nodes are out of range. Each node acts as a terminal which sends or receives data and also router in order to cooperate for communication of other nodes.

1.2 Role of group key management

Group key can be considered as a Traffic Encryption Key (TEK) which plays a vital role in secure group communication systems and have a couple of important components called as security

and efficiency [3, 4]. The security module safeguards group member authentication, group message's integrity and confidentiality, node compromise robustness, forward and backward secrecy, immediate rekeying, and group independence. The efficiency module safeguards scalability, flexibility, low storage, low computation and low communication overhead.

1.3 Trust management framework (TMF)

The "trust" concept was primarily presented by social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [5]. In the context of networking, it can be considered as the belief of an assessing node about the truthful nature of assessed node based on the experience got from past interactions. The trust characteristics are dynamic, asymmetric, context dependent, not transitive and subjective. In fact, the MANET concept works based on the cooperation among the nodes. However, due to some node exhibits selfish (i.e. save its resources without cooperating to other nodes) and malicious (i.e. populate fake routes, deny network service, drop packets, etc.) behavior leads to the necessity of a trust management framework (TMF) [6]. The purpose of TMF is to boost the collaboration in the network while penalize selfish or malicious behavior nodes. It consists of four modules, namely, trust request, trust collection, synthesize collected trust and apply the result for applications such as routing, key management, resource management, etc. The trust information collection module gathers the information about nodes' behavior from local (i.e. neighbors) nodes and recommendations from remote nodes upon sending requests [7]. The trust synthesizes module evaluates trustworthiness (i.e. how much a node can believe in other nodes) of each node based on collected information. The trust application module deduces if a node can be trusted based on its trustworthiness level.

1.4 Attacks on TMFs

We can classify the attacks posed by malicious nodes in the network into two, namely, passive and active attacks. With passive attacks, they can just copy the data traffic while with active they can modify the traffic also. To benefit from a system failure, selfish or malicious nodes can even send biased recommendations through attacks such as Black whole attack, Denial of Service attack, On-Off attack, Lying attack, Selective attack, Positional and Seasonable attacks [8, 9].

1.5 Game theory and fuzzy logic

Game theory is the concept of applied mathematics which provides mathematical tools to analyze the outcome of sequence complex decisions taken by several rational entities [10]. In the context of MANETs, it can be formally defined as a *3-tuple* game, $G = <N, A, \{ri\}>$, where $N = \{1, 2, ..., N\}$ is the set of wireless nodes in the network, A is the possible strategy chosen by each node, and for all players it is the Cartesian product, $A = A1 \times A2 \times ... \times An$, and finally ri is the reputation or payoff function $\{ri\} = \{r1, r2, ... ,rn\}$ which can get by a node if the particular strategy followed. So each node tries to maximize its reputation by choosing an optimal strategy. One of the solutions suitable in the context of MANETs for game theory is called as Nash equilibrium [11-12]. It gives a chance to get the optimal gain to all wireless nodes. No node should take its own strategy to benefit more payoffs while other node's payoffs are not improved. The Nash equilibrium is the best solution which comprises a set of strategies that nodes can choose and get corresponding payoffs.

Fuzzy logic is the concept used to handle uncertainty situations in automated artificial intelligence applications which have imprecise information and need to take decisions [13]. The result will be "degree of truth" rather than usual binary values "*true*" or "*false*". For example, the predicate, Today is sunny, might be *100%* true if there are no clouds, *75%* true if there is a slight cloud, *50%* true if it is cloudy and *0%* true if it showers all day. So instead of taking a binary decision, we will consider the options in between with this concept.

1.6 Problem Identification

There is a necessity to protect the data traffic from the internal attacks such as misbehavior or selfish node and external attacks by other competitor's due to curbs of the MANETs such as wireless medium, no central administration. In this context, most of the cryptographic algorithms which relies on group key such as symmetric and asymmetric algorithms proposed. But, these techniques involve significant computing resources and energy consumption. Moreover, these expect a central administrator, but which is lacking in MANETs. So the alternative technique proposed in the literature is called as trust based framework which significantly reduces the overhead of computation, energy required, and also resistance to attacks. Here, trust plays a vital role and the process of trust request, collect, synthesize and apply needs

significant bandwidth and energy of wireless nodes in the network. So we need a system which performs the same with less computational resources of the network without compromising security. This motivates us to work on this paper. Our proposing framework performs local optimization at each stage so that it leads to the global optimum. As far as our knowledge, no specific work considered an optimal solution at all stages like we do here. The contribution of this paperwork is to design a strategic trust management framework which would be

1. Send trust request to optimal number of nodes so that saves bandwidth and energy.
2. Trust collects from the optimal number of nodes using game theory concept.
3. Synthesize the collected trust using fuzzy logic.
4. Use irregularity pattern strategy to handle dishonest remote nodes in the network.

The rest of this paper is arranged as follows. In Section 2, the trust management frameworks proposed so far for MANETs briefed and the motivation for our work also discussed. We present our proposed optimized trust management framework in Section 3. In Section 4, we elucidate the simulation results of our proposed framework in terms of how the overhead of the network significantly reduced while maintaining security. The section 5 provides conclusions and future work aspects.

2. Related work and motivation

In the last decade or so, several trust computation models and trust based key management frameworks have been proposed for MANETs. However, the attention paid about dealing with energy saving of the wireless nodes is not up to the mark. In this section, we present the proposed models for key management and discuss their pros and cons.

In [13], the authors proposed a mechanism called as Reliable Group Key Management Framework using Fuzzy Logic for MANETs (RGMFFL). This is to detect and exclude the malicious nodes from further communication using the fuzzification and defuzzification process instead of binary classification. However, they didn't address the overhead related to the trust computation process. In [14], the authors proposed a self-organizing trust based security architecture for key management in MANETs. It works by establishing keys between nodes based on their trust level and trust relationships. The advantage of this approach is that it considers the trust as physical as well as a logical entity. However, establishing pairwise keys based on trust may not be realistic in the context of MANETS due to high scalability and network dynamics. In [15], the authors proposed a hierarchical key management framework which adopts Public Key Infrastructure (PKI) model where nodes can dynamically take management roles. It offers redundancy and robustness in the formation of Security Association (SA) between pairs of nodes. However, the certificate chains are used to derive trust relationships. In [16], the authors suggested a hop-by-hop and on-demand public key management protocol for MANETs. Here, each node makes its own public/private key pairs, issues its certificate to neighboring nodes, preserves received certificates in its certificate repository, and provides authentication service by adjusting to the dynamic network topology, without depending on a centralized server. However, the certificate chains are used to derive trust relationships.

In [17], the authors proposed a trust model based on Markov chain to get the trust values for 1-hop neighbors. They designed a trust-based hierarchical key management scheme by selecting a certificate authority server (CA) and a backup CA with the highest trust values. This work contributes a severe analysis of trust values and studies a range of attacks. However, it calculates trust, only based on direct interactions and does not consider indirect trust recommendations from remote nodes. In [18], the authors proposed a survey of key management techniques targeted to only network-layer security. In [19], the authors proposed a framework to mitigate double-face attacks based on collecting both direct and remote recommendations. However, it is not resistant to bad mouthing and iterative on-off behaviors. Here, the trust is assessed based on traffic via neighbor node and so it is time consuming.

In [20], the authors proposed a protocol independent and self-adaptive scheme named Autonomic Trust Knowledge Monitoring Scheme (ATMS). It uses autonomic management model to optimize resource consumption. However, ATMS is vulnerable to lying attacks due to there is no mechanism to separate genuine and fake trust recommendations. It is also not resistant to on-off attack due to not maintain a history of nodes. In [21], the authors proposed a multipath routing protocol for MANETs to encounter double-face attacks. However, it is vulnerable to positional attack due to recommendations are not broadcasted across the network and also weak to lying attacks. In [22], the authors proposed a dynamic nature-inspired model which calculates the trust level of nodes based on general data classes. However, the framework

cannot survive with the on-off attack and regional attacks.

In [23], the authors proposed an encryption based framework by extending AODV [24] protocol named as Trusted AODV. They used consensus algorithm to resist conflicting behavior attack. However, this framework leads to time consuming process due to the reactive nature of trust recommendations. In [25], the authors proposed trust management framework based on fuzzy logic. It combines the node's serving capability (i.e., bandwidth, remnant battery, CPU, memory, etc.) and behavior in order to compute trust. However, the performance of this approach depends on trust information collection method which is not defined clearly. It is also vulnerable to on-off attack due to not distinguishing honest and fake behaviors. In [26], the authors proposed a framework to deal with lying and double-face attacks. It evaluates the trustworthiness of a node from diverse angles such as context, severity of the outcome, etc. However, the network leads to instability due to not providing a uniform view of trust values across the network. It is immune to lying attacks, but depends on the accuracy of the methods used to evaluate the recommendations.

In [27], the authors proposed a trust-based extension of AOMDV [28] (a multi-path extension of AODV), named as Ad hoc On-demand Trusted-path Distance Vector (AOTDV) to resist bad mouthing and double-face attacks. One important observation here is that it considers the data and control packets separately. Though it is resistant to some attacks, the black list feature is a very time consuming process. A defence scheme for the recommendation based trust model is proposed in order to handle some attacks posed by dishonest recommendations, named as Cluster Based Recommendation Filtering (CBRF) [29]. It uses the clustering technique based the level of confidence, deviation threshold, and closeness centrality value to ensure that recommending node is a close friend to the evaluating node for a period of time. However, this model is heavyweight and it consumes more computing power of nodes.

In [30], the authors proposed a risk strategy model to determine the optimal number of recommendations that can satisfy the security requirements of a network. Based on the optimal number of recommendations, they introduced a new trust derivation scheme. The probability of the selected strategy was calculated based on the mixed strategy Nash equilibrium of the game. Compared with the traditional trust derivation methods, the simulation results showed that this game theoretic approach can improve the performance of the network under the premise of security assurance, especially in a dense network. But, they didn't consider the same concept for trust request, which can further improve the performance of the network.

What follows from aforesaid discussion is that the contributions made from several researchers so far mostly related to the trust computation models and mitigating the attacks on the same. A little bit work happened related to saving the computing power of a wireless node in the context of MANETs. So, we considered this issue and proposing a framework which consume less energy of the node while without compromising security..

3. Proposed framework

In this paper work we consider the MANET which consists of a set of wireless nodes with dynamic topology and there is no central administrator to monitor and control the network. Here, we adopt the work proposed in [13] and extending the same to save energy for trust computation process using soft computing technique called as game theory concept [STGM]. The network will be virtually clustered [31] just to organize the hierarchy among nodes and then the direct communication happen between nodes within the cluster, but the communication between nodes from two different clusters will be taking place via cluster leader's as shown in Fig.1. It consists of three clusters *C1*, *C2* and *C3*. Here, *N3, N7*, and *N11* are chosen as cluster leaders *CL1, CL2*, and *CL3* respectively based on their highest trust value, remaining energy and low mobility.

We assume that each wireless node has a data structure as in Table 1 and Table 2 to maintain dynamic essential information such as who are the neighbor nodes, own trust value, trust recommendation on neighbor nodes, remaining energy and its mobility rate. This information can be periodically updated through flooding. We quantify the trust as between *-1* and *+1*. The *-1* indicates that a node is completely malicious or dishonest and *+1* indicates that a node is completely genuine or honest. We consider the trust value as *0.5* for a newly joined node. The trust value of a node is figured as the mixture of direct and indirect (by remote nodes recommendations) observations as shown in Fig. 2. Here, the node *X* is evaluating node and *Y* is evaluated node. The following Eq. (1) is used to compute the trust value of a node.

$$Trust\ (N_X, N_Y) = tanh\ (T_{Direct} + T_{Recommend}) \quad (1)$$

$$T_{Direct} = (\sum_{i=1}^{n} W_i D_i) \quad (2)$$

$$T_{Recommend} = \sum_{j=0}^{m} TR_j \left(TR(N_j, N_Y)\right) \quad (3)$$

Where,

n = The no.of direct observations between X and Y.
D_i = the value between *-1* and *+1* based on the direct observation is bad or good respectively.
W_i = Weight for each direct observation based on importance.
m = The no.of remote nodes giving trust recommendations (indirect trust) on Y.
TR_j = Trust value of remote node j who sends indirect trust.
$TR(N_j, N_Y)$ = Trust value on Node Y by its neighbor's node j.

The use of the hyperbolic tangent function is to make the trust value between *-1* and *+1* despite of its value out of bounds. Here the remote nodes are R_1, R_2, and R_3 whose have direct observation with node Y. So, the node X collects trust from these remote nodes and aggregated.

We assume that there are an M number of neighbor nodes for the evaluated node. Let us consider first how the trust request process is to be optimized. Send the trust request to set of remote or neighbor nodes of the evaluated node whose trust value is above the threshold (Here, considered as *0.5*), more remaining energy (Here, considered as *5J*) and low mobility rate (Here, considered as less than *5m/Sec*). This procedure is to filter the number of remote nodes to whom the trust request sends. It saves the bandwidth of the network as well as saves energy for forwarding routing packets.

Table 1. A data structure to hold basic information about wireless nodes in network

Node (N_i)	Neighbours (N_j)	Trust (N_i)	Direct Trust on N_j by N_i
A	B, C, E	0.8	(B, A) = 0.5 (C, A) = -0.7 (E, A) = 0.2

Table 2. A data structure to hold additional information about wireless nodes in network

Node (Ni)	Remaining Energy (Ni)	Mobility Rate (Ni)
A	11 J	10 m/sec

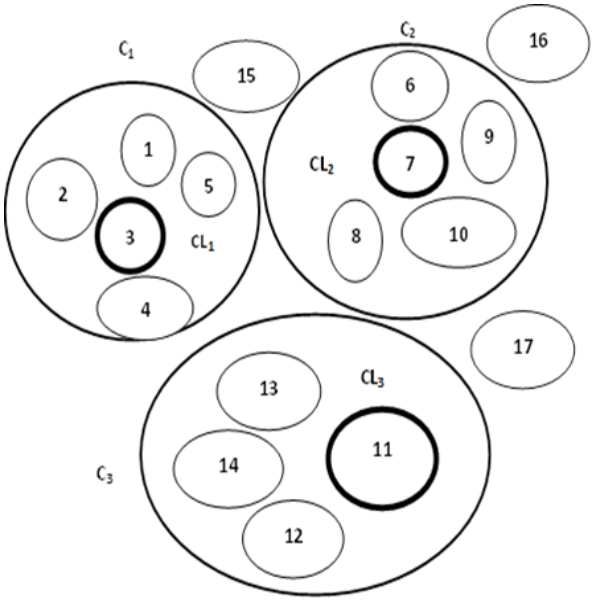

Figure.1 Formation of Clusters

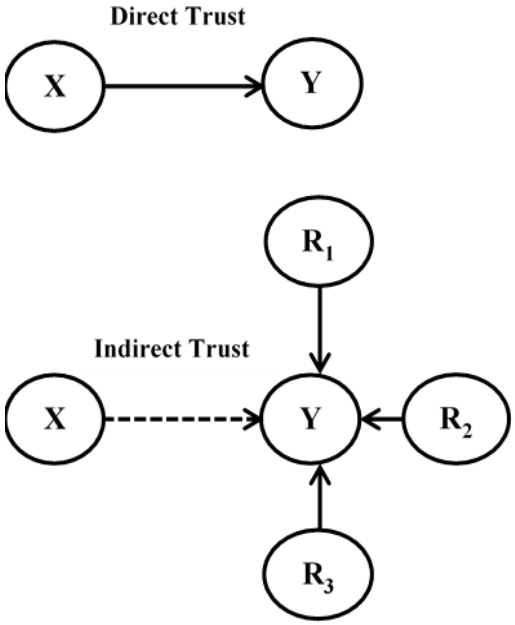

Figure.2 Computing Direct and Indirect Trust

To get the response from an optimal set of nodes the concept used in [30] is considered. We believe that the network is secure if and only if we consider all the recommendations trust into account. But, by taking the security features of the network into consideration, we define a payoff U under the condition that the number of recommending nodes that respond to the evaluating node is k. To simplify the analysis, we assume that the energy consumed by a remote node to send trust response is *Ns(e)* and assume that the corresponding gain from this task is appropriate. Consequently, we have $U > kNs(e) > 0$. Assume that the requirements of security can be fulfilled if any node sent trust response. The procedure for strategies of nodes and their payoff

matrix can be formulated in Table 3. The row player (node *i*) can be a random contributing node that receives the trust request, while the column player stands for the other *k-1* neighbor nodes.

Here, we can make a node to stop from sending the response to save energy based on the assumption that other nodes can trust honest response and they make the network work. As a random node chooses its own strategy, all the wireless nodes are independent in this game. We assume that a random node *i* send a trust response with probability *p*, or remains stopped with probability *1-p*. Then out of *k* nodes, at least one node replies the trust request with a probability of $1-(1-p)^{k}$. As a result, the mixed strategy Nash equilibrium can be computed by Eq. (4) and consequently, the probability of sending trust reply *p* can be computed and then *q = (1-p)* will be computed.

$$U\,(1-(1-p)^{k-1}) = U - Ns(e) \quad (4)$$

Once the direct and indirect trust gathered together, the final mixture will be synthesized further using fuzzy logic instead of taking a binary decision. The Table 4 describes about the working model of synthesizing module in the trust management framework using a fuzzy logic system with Rule base (i.e. IF-THEN control structures) to eliminate recommendations from dishonest nodes from the network to avoid further communication with those nodes.

Table 3 Payoff Matrix for any one node sends a response (*k=1*)

For (k=1)		**Other Remote Nodes (M -1)**	
		No Other Response	**At Least One Response ($1 \leq \beta \leq M-1$)**
Node Ni	**No Response**	*0,0*	*U, U – β Ns(e)*
	Response	*U – Ns(e) , U*	*U – Ns(e) , U – (β Ns(e))*

Table 4 Fuzzy Set Membership Function

Trust value of a node	**Trustworthiness of a node**	**Recommendation risk of a node**
0.5 to +1	Excellent	NIL
0 to 0.49	Very Good	Low
-0.6 to -0.99	Good	Moderate
-0.3 to -0.59	Fair	High
-1 to -0.29	Poor	Very High

The pattern irregularity in the recommendations will be checked in order to handle the on-off attack in which the malicious nodes behavior will switch between normal (honest recommendations) and abnormal (dishonest recommendations) over a span of time. We maintain the history of the recommendations made by remote assessing nodes on a particular assessed node, didn't consider the recommendations which are too far from the variance and then taking into account the average of all that. So, it will not affect much on the trust value of a node in particular duration. The proposed optimal trust management framework follows the below steps periodically.

1. *Initialize the Network.*
2. *if Node Ni is ready then*
3. *flood the basic information to all nodes in the Network.*
4. *end if*
5. *Form the Clusters and Select the Cluster Leader's.*
6. *One of the Cluster Leader CLi initiates the trust computation periodically.*
7. *To collect indirect trust for node Nj by Ni*
8. *Ni sends trust request to only set of neighbor nodes (M) whose trust value is above threshold (Trust (Ni) > Threshold), high remaining energy and Low Mobility.*
9. *Select optimal k < M, which is sufficient to recommend trust instead of all neighbor's.*
10. *Compute the final trust based on Direct and Indirect trust.*
11. *Synthesize the calculated trust value based on following Fuzzy Rules:*
12. *If (Trustworthiness(Ni) is Excellent) Then Recommendation_Risk(Ni) is NIL*
13. *If (Trustworthiness(Ni) is Very Good) Then Recommendation_Risk(Ni) is Low*
14. *If (Trustworthiness(Ni) is Good) Then Recommendation_Risk(Ni) is Moderate*
15. *If (Trustworthiness(Ni) is Fair) Then Recommendation_Risk(Ni) is High*
16. *If (Trustworthiness(Ni) is Poor) Then Recommendation_Risk(Ni) is Very High*
17. *Select the Cluster Leader based on latest trust values.*
18. *Repeat step 2 to 18 periodically.*

4. Simulation and results

4.1 Simulation settings

To simulate our proposed framework, we used NS2 simulator [32] tool which is an open source discrete event simulator exclusively designed to promote research in the field of computer networks

including MANETs. We used the Multicast AODV routing protocol in order to benefit from multicasting feature. The network is simulated in the area of 1000 X 1000 square meters with 100 mobile nodes with simulation time is 500Secs. The network configuration settings are shown in Table 5. In order to test the network performance with the proposed trust management framework, we considered metrics such as Packet Delivery Ratio, Packet Loss, Residual Energy, Detection Ration of malicious nodes, and Group Key Management Overhead in the cases of our proposing work, STGM and existing framework named as RGMFFL [13]. The results are plotted from Fig. 3 to Fig. 7. We assumed that there are maximum 60% of malicious nodes (dishonest recommending nodes) in the network and the percentage of malicious nodes is increased to the maximum level during the span of simulation time, 500Secs. It is witnessed that the network packet delivery ratio with STGM at in the range of 88% to 70%, while with RGMFFL framework the same falls from 88% to 28%. This improvement is because of the elimination of malicious nodes by discriminating them by degree of trustworthiness of the nodes predicted through fuzzy classification. The fuzzy classifier helps to find the group of lowest trustworthy nodes with highest elimination risk. Here, the detection ratio of malicious nodes has been increased over the simulation time and so there is a significant increase in the packet delivery ratio and decrease in packet loss. As we are also maintaining the history of recommendations given by a remote node on a particular node, the mean value of the trust will be considered as final. It helps to avoid the too far away recommendations from the remote nodes.

Table 5. Simulation Settings

Number of Nodes	100
Area	1000 X 1000 square meters
MAC	802.11
Simulation Time	500 Sec
Traffic Source	CBR
Mobility Model	Random Waypoint
Speed	10 m/Sec
Pause Time	50 Sec
Routing Protocol	MAODV
Initial Energy	15 J
Trust Threshold	0.3
Radio Range	200 m
Propagation	Two-ray ground reflection model

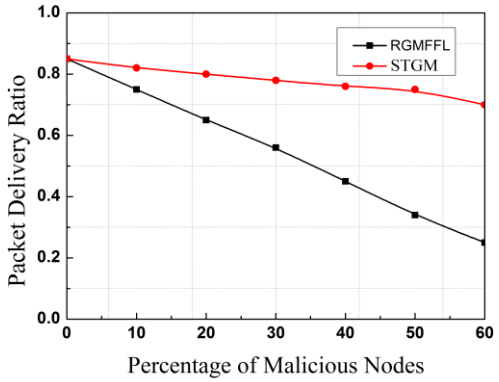

Figure.3 Malicious nodes Vs packet delivery ratio

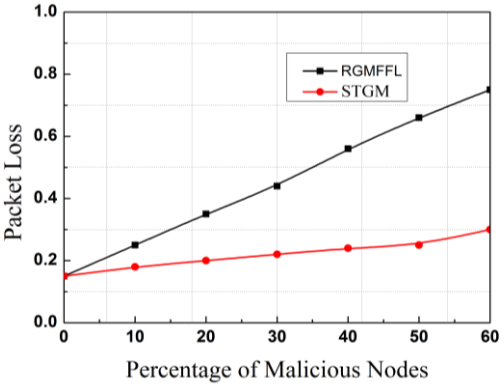

Figure.4 Malicious nodes Vs packet loss

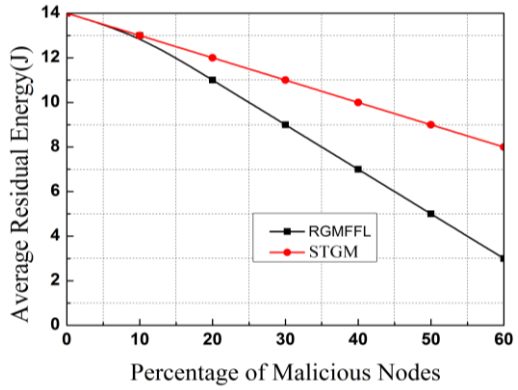

Figure.5 Malicious nodes Vs average residual energy

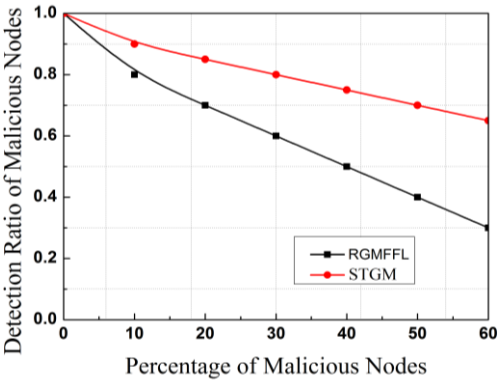

Figure.6 Malicious nodes Vs detection ratio of malicious nodes

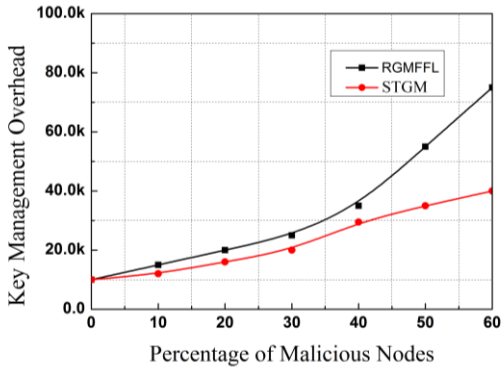

Figure.7 Malicious nodes Vs key management overhead

It is also observed that the percentage of packet loss without optimized framework upsurges while reduced significantly with optimized framework. To simulate the residual energy of nodes we considered the average of all the nodes in the network. The behavior of energy consumed by wireless nodes in the MANET has fallen from 14J to almost 8J with our proposed framework, STGM and while the same fallen from 14J to nearly 2J with the existing RGMFFL framework. The energy saved due to send the trust request itself to a subset of the nodes among all neighbors without compromising the security of the network. This is because with the help of game theory concept called as Nash equilibrium; we will get the optimal (necessary and sufficient) subset of the nodes that will send the response to the trust request from assessing node on assessed node. So the bandwidth of the network saved as well as the energy of the remaining nodes will be saved without receiving requests and responding to the same.

The detection ratio of malicious nodes is in the range of between 100% and 70% with our framework, STGM and while the same is between 100% and 30% with the existing RGMFFL framework. This is because of the fuzzy classifier which will get the degree of genuineness and do the classification between honest and dishonest nodes. Further the rate of detection of malicious nodes is decreased due to the remote nodes are colluding together to avoid from the detection by fuzzy classifier. The key management overhead is observed as the number of control packets used. Almost 40% of significant key management overhead is reduced with our proposed framework while comparing to the existing framework. There are three reasons for the significant reduction in the key management overhead. The first one is that we are sending the request to the nodes whose trust value is excellent and has more energy. The second one is to get the response from a subset of the nodes only. So the number of control packets will be saved and so the overhead of the network will be saved for each time of the re-keying process due to a new node joins into the network or an existing node left of the network.

4.2 Security threat model

For testing the proposed security framework, we have launched outsider attacks such as replay attack, node capture attack, data manipulation attack and selective forwarding attacks. This approach considers the insider attacks such as the Packet dropping attack, false trust report attack, report disruption attack, false join or leave requests, battery exhaustion attack (DDoS). Because of using key management and authentication, outsider attacks are avoided from the network. By using the trust mechanism, insider attacks are also detected and prevented. To simulate about the handling of internal attacks, let us consider the network with 20 nodes with 3 clusters virtually. Assume the corresponding trust values of nodes and their clusters are as shown in the Table 6.

Let us consider the source *S = Node 3* and destination *D = Node 20*. Let *P1, P2* and *P3* be the possible routes determined for *S* to *D* given by

P1 => 3-2-9-11-14-17-20
P2 => 3-2-7-11-12-14-20
P3 => 3-2-9-11-10-16-17-20

Let TRP1, TRP2 and TRP3 be the total global trust values of the paths P1, P2 and P3, respectively, given by

Table 6. Global Trust values of all nodes

Node id	Cluster Id	Global Trust value (TR)
1	C1	0.40
2	C1	0.70
3	C1	0.54
4	C1	0.64
7	C1	0.33
8	C2	0.74
9	C2	0.42
10	C2	0.28
11	C2	0.81
12	C2	0.23
13	C2	0.69
14	C3	0.52
15	C3	0.45
16	C3	0.75
17	C3	0.81
18	C3	0.48
20	C3	0.65

TRP1 =
0.54+0.70+0.42+0.81+0.52+0.81+0.65 =4.45
TRP2 =
0.54+0.70+0.33+0.81+0.23+0.52+0.65 =3.78
TRP3 =
0.54+0.70+0.42+0.81+0.28+0.75+0.81+0.65 =4.15

Hence the path *P1* which is having the highest global trust value (*4.45*) is selected, whereas the paths *P2* with least trust value (*3.78*) and *P3* with less trust value (*4.15*) are not selected, thereby omitting the internal attacker's nodes *7, 10* and *12*.

5. Conclusion and future works

In this paper, we proposed a soft-computing based trust management framework for handling the process of group key management in the MANETs. Here trust value is determined for each node based on the direct and indirect observations. In this context, the trust request and collection plays a vital role and so leads to the overhead of the network. To minimize the same we applied the concept of game theory to send the trust request itself to the subset of the remote nodes whose responses are necessary and sufficient without affecting the security of the members in the network. The concept of Nash equilibrium gives the best strategy to choose at every time of trust calculation and so saving the bandwidth of the network and energy of the nodes. Later the trust value of all nodes would be interpreted with fuzzy classifier in order to find the group of lowest trustworthy nodes whose elimination risk at very high. Those nodes will be excluded from further communication in the network. Then, the network is clustered and the cluster leader is elected based on the highest trust vale, highest remaining energy and lowest mobility rate. The working mechanism of the proposed framework described through an algorithm. By simulation results, we proved that the proposed technique reduces the number of control packets required to manage a group key and so leads to save energy of each node during the re-keying process. A weakness of using fuzzy logic is that storing the rules database might involve a significant amount of memory. It is also good if it has a mechanism to evade from isolating remote alone nodes. As a future work direction, we plan to investigate aforementioned issues and defence mechanisms for attacks such as bad-mouthing, ballot-stuffing, and collusion posed by dishonest nodes.

References

[1] K.K. Chauhan and A.K. Singh Sanger, "Securing mobile ad hoc networks: key management and routing", *International Journal on Ad Hoc Networking Systems*, Vol. 2, No. 2, 2012.

[2] S. Rafaeli S and D. Hutchison D, "A survey of key management for secure group communication", *ACM Computing Surveys*, Vol. 35, No. 3, pp. 309–329, 2003.

[3] O. Cheikhrouhou, "Secure group communication in wireless sensor networks: a survey", *Journal of Network and Computer Applications*, Vol. 61, pp. 115-132, 2016.

[4] G Nagaraja and Pradeep Reddy CH, "A survey on group key management frameworks for secure group communication in mobile ad hoc networks", *International Journal of Pharmacy & Technology*, Vol. 8, pp. 4121-4129, 2016.

[5] Karen S. Cook, "Trust in society," *1st ed. New York: Russell Sage Foundation*, 2001.

[6] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks", *IEEE Communications Surveys & Tutorials*, Vol. 13, pp. 562–583, 2011.

[7] X. Li, J. Slay, and S. Yu, "Evaluating trust in mobile ad hoc networks," *In: Proc. of the International Conference on Computational Intelligence and Security*, pp. 1-10, 2005.

[8] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey", *IEEE Communications Surveys & Tutorials*, Vol. 18, pp. 1287-1309, 2016.

[9] G. Nagaraja and Pradeep Reddy CH, "Mitigate lying and on-off attacks on trust based group key management frameworks in MANETs", *International Journal of Intelligent Engineering and Systems*, Vol. 9, No.4, pp. 215-224, 2016.

[10] C. Kamhoua, N. Pissinou, and K. Makki, "Game theoretic modeling and evolution of trust in autonomous multi-hop networks: application to network security and privacy", In: *Proc. of the IEEE International Conference on Communications*, pp. 1–6, 2011.

[11] M. Naserian and K. Tepe, "Game theoretic approach in routing protocol for wireless ad hoc networks", *Ad Hoc Netw.*, Vol. 7, No. 3, pp. 569–578, 2009.

[12] L. Dasilva, H. Bogucka and A. Mackenzie, "Game theory in wireless networks", *IEEE Communications Magazine*, Vol.49, No.8, pp.110-111, 2011.

[13] G. Nagaraja and Pradeep Reddy CH, "A Reliable Group Key Management Framework Using Fuzzy Logic for MANETs", I*nternational Journal of Intelligent Engineering and Systems*, Vol.9, No.4, pp.107-115, 2016.

[14] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying Trust in Mobile Ad-Hoc Networks", In: *Proc. of the Int'l Conf. Integration of*

Knowledge Intensive Multi-Agent Systems, pp. 65-70, 2005.

[15] G. C. Hadjichristofi, W. J. Adams, and N. J. Davis, "A Framework for Key Management in a Mobile Ad Hoc Network", In: *Proc. of the Int'l Conf. on Information Technology: Coding and Computing, Tiejun Huang*, Vol. 2, pp. 568-573, 2005.

[16] R. Li, J. Li, P. Liu, and H. H. Chen, "On Demand Public Key Management for Mobile Ad Hoc Networks", *Wiley's Wireless Communications and Mobile Computing*, Vol. 6, No. 3, pp. 295-306, 2006.

[17] B. J. Chang and S. L. Kuo, "Markov Chain Trust Model for Trust Value Analysis and Key Management in Distributed Multicast MANETs", *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 4, pp. 1846-1863, 2009.

[18] A. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure and P. Spilling, "A Survey of Key Management in Ad Hoc Networks", *IEEE Commun. Surveys and Tutorials*, Vol. 8, No. 3, pp. 48-66, 2006.

[19] G. Bella, G. Costantino, and S. Riccobene, "Managing reputation over MANETS," *In: Proc. of the 4th Int. Conf. Inf. Assur. Security*, pp. 255–260, 2008.

[20] Z. Movahedi, M. Nogueira, and G. Pujolle, "An autonomic knowledge monitoring scheme for trust management on mobile ad hoc networks", In: *Proc. of the IEEE Wireless Communications and Networks Conf.*, pp. 1898–1903, 2012.

[21] S. Almotiri and I. Awan, "Trust routing in MANET for securing DSR routing protocol," *PGNet*, 2010.

[22] M. Seredynski and P. Bouvry, "Nature-inspired evaluation of data classes for trust management in MANETS", In: *Proc. of the IEEE 26th Int. Parallel Distributed Processing, Symposium, Workshops & PhD Forum*, pp. 366–373, 2011.

[23] X. Li, M. R. Lyu, and J. Liu, "A trust model based routing protocol for secure ad hoc networks," In: *Proc. of the IEEE Aerosp. Conf.*, Vol. 2, pp. 1286–1295, 2004.

[24] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing", In: *Proc. of the 2nd IEEE Workshop Mobile Comput. Syst. Appl.*, pp. 90–100, 1977.

[25] H. Xia, Z. Jia, L. Ju, X. Li, and Y. Zhu, "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules", In: *Proc. of the IEEE/ACM Int. Conf. Green Computing Communications*, pp. 124–130, 2011.

[26] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach", In: *Proc. of the 11th Int. Conf. Mobile Data Manage.*, pp. 85–94, 2010.

[27] X. Li, Z. Jia, L. Wang, and H. Wang, "Trust-based on-demand multipath routing in mobile ad hoc networks," *IET Inf. Security*, Vol. 4, No. 4, pp. 212–232, 2010.

[28] Y. Yuan, H. Chen, and M. Jia, "An optimized ad-hoc on-demand multipath distance vector (AOMDV) routing protocol", In: *Proc. of the Asia-Pac. Conf. Commun.*, pp. 569–573, 2005.

[29] A.M. Shabut, K.P. Dahal, S.K Bista, and I.U. Awan, "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs", *IEEE Transactions on Mobile Computing*, Vol. 14, No. 10, pp. 2101–2155, Oct. 2015.

[30] J. Duan, D. Gao, D. Yang, C.H. Foh, and H.H Chen, "An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications", *IEEE Internet of Things Journal*, Vol. 1, No. 1, 2014.

[31] K. Drira, H. Seba, H. Kheddouci, "ECGK: An efficient clustering scheme for group key management in MANETs", *Computer Communications*, Vol.33, pp.1094–1107, 2010.

[32] T. Issariyakul and E. Hossain, Introduction to Network Simulator NS2. *New York, NY, USA, Springer*, 2011.