INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Mitigate Lying and On-Off Attacks on Trust Based Group Key Management Frameworks in MANETs

G Nagaraja[1*] **Pradeep Reddy Ch**[2]

[1]*SITE, VIT University, Vellore, India*
[2]*SITE, VIT University, Vellore, India*
* Corresponding author's Email: nagaraja.g@vit.ac.in

Abstract: Instant collaborative group communication can be achieved by deploying Mobile Ad Hoc Networks (or MANETs) without any pre-plan and pre-existing infrastructure setup. However, the curbs thrown by these networks, motivate the necessity of a group key management framework to secure data traffic. In this context, significant research work done in the last decade and proved that the trust based frameworks deliver better performance than others. In MANETs, trust quantified as the belief held by a node about another node. It is evaluated based on the assessing node direct experiences with assessed node itself, if they are neighbors and recommendations from remote nodes in the network with which assessed node has a direct experience, if they are remote. However, the framework based on recommendations by other nodes in the network might ultimately lead to system failure due to the menace of unfair recommendations by selfish and malicious nodes. Lying and on-off attacks on the system are such type of attacks. This motivates us to work on a framework which is immune to aforesaid attacks and should be lightweight due to node's has limited computing resources. We propose a framework which scrutinizes dishonest recommendations based on the trust threshold value of remote nodes, distance from mean of trust recommendations and by maintaining a history of recommendations. Our simulation outcomes prove that proposed framework can deliver better network performance and resistance to lying and on-off attacks.

Keywords: Secure Group Communication, Group Key Management, Trust, Mobile Ad Hoc Networks, Lying attack, On-Off attack.

1. Introduction

1.1 Mobile Ad Hoc Networks

A Mobile ad hoc network (or MANET) is a wireless network consists of mobile nodes which require trivial or infrastructure-less to deploy and communicate, and has a dynamic topology due to a node may join into, leave from, or move around the network at any point of time [1]. Since a MANET can be quickly and spontaneously arranged, it has intensified attractiveness in collaborative application scenarios such as disaster rescue operations, battlefields, conferences, etc. The majority of these setups expect an efficient and secure group communication framework [2]. The obstacles to build such framework in MANETs include limited computing power (i.e. Bandwidth, Battery, CPU, Memory, etc.), untrustworthy wireless medium and regular changes of network topology brought by node mobility. In a MANET, there is a direct communication between neighbors within the range of wireless medium or 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 also called as Traffic Encryption Key (TEK) which plays a vital role in secure group communication systems and has two important modules called as security and efficiency [3]. The security module ensures group member authentication, group message's integrity and confidentiality, node compromise robustness, forward and backward secrecy, immediate rekeying, and group independence. The efficiency module ensures scalability, flexibility, low storage, low computation and low communication overhead.

1.3 Trust Management Framework (TMF)

The "trust" concept was initially introduced by social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [4]. 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) [5]. The purpose of TMF is to boost the collaboration in the network while penalize selfish or malicious behavior nodes. It consists of three key modules, namely, trust information collection, trust level computation and trust establishment. The trust information collection module gathers the information about nodes' behavior from local (i.e. neighbors) nodes and recommendations from remote nodes. The trust computation module evaluates trustworthiness (i.e. how much a node can believe in other nodes) of each node based on collected information. The trust establishment module deduces if a node can be trusted based on its trustworthiness level.

1.4 Attacks on TMFs

To benefit from a system failure, nodes can send unfair recommendations through attacks such as Lying attack, On-Off attack, Selective attack, Positional and Seasonable attacks [6]. This classification is based on how the attack misleads the trustworthiness assessment of a node about another node.

Lying attack: It involves sending dishonest recommendations about other nodes by broadcasting false claim that a good node is malicious or boosting trust values for actual misbehaving nodes.

On-Off attack: It means sending dishonest or honest recommendations alternatively by switching between misbehavior (on) or normal (off) manners respectively.

Selective attack: The nodes act as dishonest about particular victim nodes and behave honestly about other nodes.

Positional attack: The nodes behavior (sending honest or dishonest recommendations) varies based upon the position or region at which it is working on the network.

Seasonable attack: The nodes behavior varies based upon the time at which it is working on the network. Sometimes sends honest information and sometimes sends dishonest information.

1.5 Problem Identification

As per the aforementioned discussion, trust based frameworks based on the recommendations are vulnerable to some attacks posed by malicious or selfish nodes in the network. The system may leads failure due to unfair evaluation of the trustworthiness level of each node. This motivates us to work on this issue and we propose a framework which is immune to attacks up to a certain extent. Our framework scrutinizes dishonest recommendations based on the trust threshold value of remote nodes, distance from mean of trust recommendations and by maintaining a history of recommendations. The contribution of this paper is to design and develop a framework which should be

a. Lightweight which consumes less computing resources, such as energy, memory, CPU time, etc.

b. Immune to Lying attack.

c. Immune to On-Off attack.

The remainder of this paper is structured as follows. In Section 2, we brief various trust management frameworks proposed so far for MANETs and the motivation for our proposal. We present an overview of the proposed framework with key principles to be followed in order to handle dishonest recommendations in Section 3. In Section 4, we elucidate the implementation and results of our proposed framework by comparing among without any defence scheme, with existing work and proposed framework. Conclusion and future work remarks are in section 5.

2. Related Work and Motivation

In the last decade or so, various trust computation models and trust based key management frameworks have been proposed for MANETs. However, the attention paid about dealing with attacks based on lying recommendations by malicious 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 [7], 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 [8], 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 [9], 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 [10], 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 [11], the authors proposed a survey of key management techniques targeted to only network-layer security. In [12], the authors proposed a framework to mitigate double-face attacks based on collecting both direct and remote recommendations. This framework is strong to conflicting behavior and on-off attacks with little extra overhead. 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 [13], 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 [14], 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 [15], 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 [16], the authors proposed an encryption based framework by extending AODV [17] 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 [18], the authors proposed trust management framework based on fuzzy logic [19]. 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 [20], 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 [21], the authors proposed a trust-based extension of AOMDV [22] (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) [23]. It uses the clustering technique and based on three parameters: (a) the level of confidence held by a node about others, (b) deviation threshold which ensures the unity of views between evaluating node and the evaluated node, and (c) 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.

What follows from aforementioned debate is that mitigating or eliminating the consequences of malicious behavior is still an interesting problem in the context of MANETs. So, we considered this issue and proposing a framework which is immune to aforesaid attacks up to some extent.

3. Proposed Framework

In this section, we present the working model of our proposed framework in a step-by-step manner. We use cluster based trust management framework [24] in order to make the system as lightweight. The pros of clustering method are only the nodes which are in cluster affects (re-keying [25] will be done within a cluster), if any node joins into or leave (due to mobility or self-exit) from that cluster. The other nodes within other clusters would not disrupt. It saves the computing resources of nodes. The Figure 1 depicts our proposed framework.

3.1 Trust Evaluation

We quantify the trust of node as a continuous real value between *-1* and *+1*. The *-1* indicates that a node is absolutely malicious and *+1* indicates that a node is absolutely honest. We consider the trust value as *0* for a newly joined node. The trust value of a node is computed as the combination of direct and indirect (through remote nodes) experiences as shown in Figure 2.

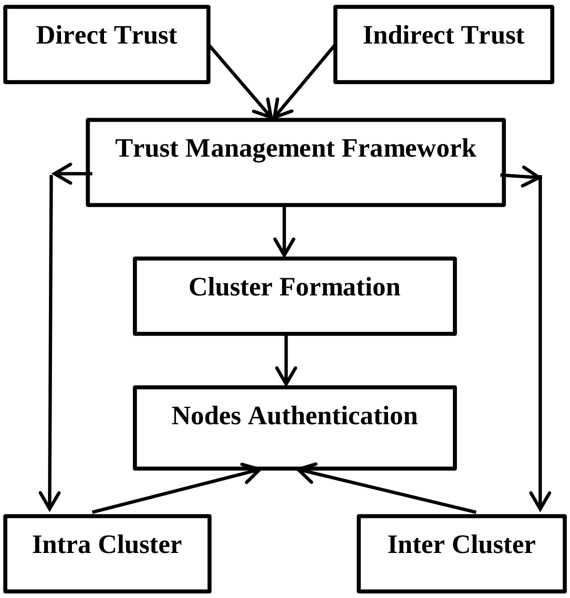

Figure.1 Proposed Trust Management Framework

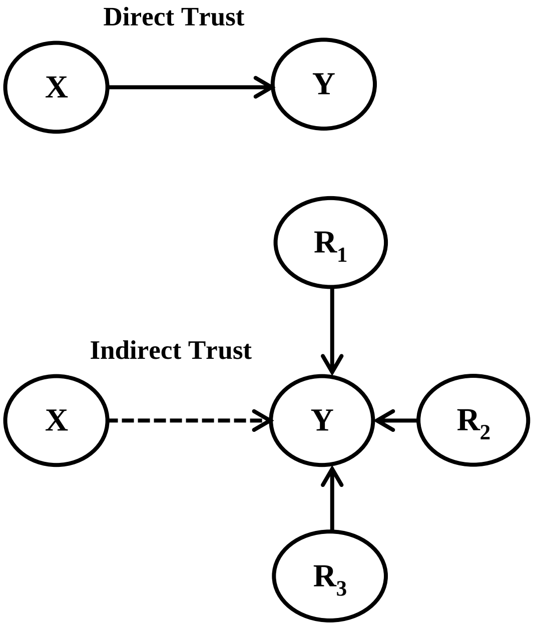

Figure.2 Proposed Trust Management Framework

Here, the node X is assessing node and Y is assessed node. The following equation (1) [26] is used to compute the trust value of a node.

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

$$T_{Direct} = \left(\sum_{i=1}^{n} W_i * D_i \right) \tag{2}$$

$$T_{Recommend} = \left(\sum_{j=1}^{m} TR_j * \left(TR(N_j, N_Y) \right) \right) \tag{3}$$

Where,

n = The no.of direct experiences between X and Y.
D_i = Either -1 or +1 based on the direct experience is negative or positive respectively.
W_i = Weight for each direct experience.
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 purpose of the hyperbolic tangent function is to make the trust value between *-1* and *+1* even though it is out of this boundary. The direct trust is computed based on the direct experience with assessed node by assessing node, if they are neighbors; otherwise the indirect trust recommendations will be collected from the remote nodes that are having direct experience with assessed node and aggregated [27]. Here R_1, R_2, and

R_3 are remote nodes who have direct experience with node *Y*. So, the node *X* gathers trust information from these remote nodes and aggregated. The aggregate function works based on the following three principles and these are the core component of our proposed work.

1. Some trust recommendations collected from the remote nodes whose trust value is less than the threshold value (Here, it is *0*) will be treated as lying recommendations from malicious nodes. It helps to reduce the impact of untrustworthy recommendations from dishonest nodes and leads to prevent lying attacks
2. If the trust recommendation value is too much distance from the average of trust recommendations from all nodes on the assessed node, then those recommendations also treated as lying recommendations from malicious nodes. It helps to reduce the impact of untrustworthy recommendations from a group of dishonest nodes and leads to prevent lying attacks.
3. In order to mitigate the On-Off attack, we will maintain the history of recommendations made by neighbor's nodes for each node over a period of time. We consider the average of the entire history of recommendations and so it leads to prevent On-Off attack.

3.2 Evaluation of node mobility

The mobility for each node *j* with respect to node *i* (M_i^j)) is evaluated by computing the ratio of received signal strength (*RSS*) among the two successive data transmissions from a neighbor node. It is defined by the following equation (4) [28].

$$M_i^j = 10 \, log10 \, \frac{RSS_{i \to j}^{new}}{RSS_{i \to j}^{old}} \qquad (4)$$

Where,

$$RSS - \beta * \vartheta * Ptx \qquad (5)$$

β - It is constant which depends on the antennas and the wavelength

ϑ - The gain of the channel

Ptx = The transmitter signal power.

3.3 Storing Cluster and Trust Information

Table 1. Neighbor's and Cluster information

Node Id	Neighbor's	Cluster No	Cluster Head
N_i, *i*= *1*to *n*	N_j, *j* = *1* to *m*	C_k, *k*= *1* to *c*	CH

Table 2. Trust Information Table

Node Id	Trust Value
N_i, *i* = *1*to *n*	Between -1 and 1

Table 3. Trust Information Table

Node ID	Trust Value (TR_i)	Number of Hop (H)	Mobility Value

Table 4. Format of RREQ message

Source ID	Destination ID	Trust Information	
		N_i	TR_i

Each node maintains two tables, namely Neighbor's and Cluster information and Trust Information table. The formats of both tables are shown in Table 1 and Table 2. The neighbor's and cluster information table has the information about the all neighbor's of a node and its cluster head information. The trust information table contains the trust value of each node within the network. Both tables will be periodically updated while the network is in execution mode.

3.4 Formation of Clusters

The following procedure will be used to form the clusters in the network.

a. When the nodes are deployed in the network, it broadcasts the hello message to its neighboring nodes (*Neighibor*).
   N_i → *Neighibor: Hello*. The format of *Hello* message is shown in Table 3. The trust value and mobility are evaluated as per the discussions in sections 3.1 and 3.2 respectively.
b. Based on the *Hello* message, each N_i identifies itself and also maintains the neighbor list ($N_{Neighbor}$).
c. N_i declares itself as the cluster head (*CH*) based which has highest trust value and lowest mobility.
d. Once N_i is declared as *CH*, it updates its identity in the *CH* field of its hello messages

and sets the *H* field of these messages as 'zero'.

e. All $N_{Neighbor}$ which contains the trusted relations with *CH* joins the cluster. Its *Hello* message contains the identity of *CH* in the *CH* field and *H* field of these messages as 'one'. If a node *Ni* has trusted relationship with several *CHs* then it chooses the *CH* with maximum TR_i.

f. If there exist some nodes without joining the cluster and it holds the trust relation with at least one cluster, then it joins the cluster with maximum trust value.

3.5 Transmission of Data

The procedure involved in data transmission in the network is as follows. Let *S* and *D* be the source and destination respectively.

a. When *S* wants to transmit data packet to *D*, it broadcasts a route request packet (*RREQ*) on a control channel. The format of *RREQ* packet is shown in Table 4.

b. When an intermediate node receives the *RREQ* packet from *S*, it verifies its route cache whether it has already forwarded the same packet, if common channels exist with the sender node or trust value is significantly less. If either of the condition is satisfied, then N_i drops the packet; otherwise appends the identifiers to the partial path, adds TR_i to its trust value and broadcasts updated *RREQ* to its neighbors.

c. When *D* receives *RREQ* packets, it selects the route with maximum trust value.

d. *D* then generates the *RREP* packets, copies the route records from *RREQ* and sends it back to *S* on the reverse path.

e. *S* after receiving *RREP* packets estimates the trust value.

In order to prevent the internal attacks, *S* chooses the path with maximum trust as best primary routing path. The next maximum trusted path is chosen as the secondary routing path. Then it transmits the data packet to *D* through the chosen paths.

3.6 Inter and Intra Cluster Authentication

Here, we brief the procedure for intra-cluster and inter-cluster source authentication performed by the selected trusted cluster heads (*TCHs*).

3.6.1 Inter-Cluster Authentication

Let *TTP* be the offline trusted third party (*TTP*). Let *S* generate a pool of *W* keys. Let *O* keys be the share of *W* keys. The procedure is as follows.

a. Once the trusted cluster heads (*TCH*) are selected, it sends a registration request (*RG_REQ*) to *TTP*.

$$TCH \xrightarrow{RG\_REQ} TTP$$

b. *TTP* upon receiving *RG_REQ* message transmits a secret key (*B*) to each *TCH*.

c. When *S* wants to transmit a multicast data packet (*DP*), it will first inquire the set of registered *TCH* with the *TTP*.

d. The *TTP* will transmit the details of registered *TCH* and the secret key.

e. *S* then allocates a share of *O* keys for each *TCH* among the pool of *W* generated keys by encrypting with the secret key obtained from *TTP*. Here, $W < O^*$, number of clusters in the network.

f. Each *TCH* obtains its share of keys by decrypting with the secret key.

g. *S* appends multiple Message Authentication Codes (*MACs*) to the multicast packet (*MCP*). Each *MAC* is related to distinct key.

h. During broadcast, set of *W MACs* will be included in a packet.

i. *S* then transmits a multicast message to *TCH*.

j. Each *TCH* checks the *MACs* and confirm the source authenticity when a set of *O MACs* in the message are found to be based on *O* keys assigned to *TCH* by *S*.

Here, the values *W* and *O* are subject to trade-off between security and bandwidth overhead. Moreover, the issue of key share to the cluster heads will be secure and avoids capture of shared keys by any attacker.

3.6.2 Intra-Cluster Authentication

In order to communicate users with each other within the cluster, they need to have the common cluster group key. It involves the following process:

a. *S* generates a chain of one-time-use keys using the hash function, and shares only that last generated key, R_l, with the receivers.

b. To verify the authentication key, the receiver recursively applies the cryptographic hash function until reaching R_l.

c. If the key is already being used before, the receiver node stops applying the hash function.
d. Before delivering the multicast data to the group members, *S* evaluates the trust values of the intended receivers. Only trusted receivers are allowed to get the data.
e. *S* then encrypts the data with the R_1 and transmits it to the trusted recipient.
f. The receiver node uses the hash function to decrypt the received data.

Here, the message can be authenticated only when the used key in the chain is revealed. Also, a key cannot be used more than the pre-defined time duration and relevant message will be ignored if the *MAC* is related to expired keys.

4. Simulation and Results

4.1 Simulation Settings

To simulate our proposed framework, we used NS2 simulator [29] 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. The simulation time is 500 s and pause time is 50s. The network configuration setting is shown in Table 5.

4.2 Simulation of Network Performance

In order to measure the network performance with trust management framework, we considered metrics as network Packet Delivery Ratio, Packet Loss and Energy in the presence of dishonest recommending nodes [30]. We assumed there may be maximum 60% of malicious nodes (dishonest recommending nodes) in the network and tested the performance of the network without any defence framework (WADF), with our proposed framework (WPF) and CBRF [23] model. The results are shown in Figure 3 and Figure 4.

It is witnessed that the network packet delivery ratio without any defence framework tumbles from 85% to 25%, while the percentage of malicious nodes increased from 0% to 60%. However, with our proposed framework, it maintains nearly 80% of packet delivery ratio compared with CBRF in which falls to 70%, even though the percentage of malicious nodes increased over a span of time. It is also observed that the percentage of packet loss without any defence framework upsurges while increasing the percentage of malicious nodes from 0% to 60%. However, with our proposed framework, it maintains nearly 25% of packet loss compared with CBRF in which rises to 40%, even though the percentage of malicious nodes increased over a span of time. The behavior of energy consumed by our proposed framework and CBRF is simulated in Figure 5 and the results proved that our framework is lightweight compared to CBRF. The performance of Packet Delivery Ratio and Packet Loss are due to not taking into account about the recommendations given by remote nodes whose trust value is less than the threshold value. Due to the simple set of rules as compared to the complex mechanism in CBRF defined for avoiding dishonest recommendations, the proposed framework consumes less energy (or computing power) for each node.

Table 5. Simulation Settings

Number of Nodes	100
Area	1000 X 1000 square meters
MAC	802.11
Simulation Time	500 Sec
Traffic Source	CBR
Number of Attackers	Between 0% and 60%
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

4.3 Simulation of Lying Attack

To simulate the influence of lying attack, we assumed the range of malicious nodes from 0% to 60% and assumed both positive and negative weightage for node behavior and so the trust value ranges from -1 to 1. We tested how a node trust value affects based on false negative (dishonest recommendations on a good node) and false positive (dishonest recommendations on a bad node) actions by malicious nodes. We considered node’s 35 for former case and node’s 70 for later case. The results are shown in Figure 6 and Figure 7. It is witnessed that without any defence scheme, the node trust value will be upsurge or decrease because of fake recommendations. However, our proposed framework maintains nearly the constant trust value 0.7 and -0.7 for a good and bad node’s respectively, compared with CBRF even though the percentage of malicious nodes increased over a span of time. This performance is due to not considering the outlier nodes recommendations (i.e. which are far away from the mean) as well as avoiding recommendations from whose trust values are low. So the node’s trust values will not affect from dishonest recommendations.

4.4 Simulation of On-Off Attack

In the on-off attack, the malicious nodes behavior will switch between normal (honest recommendations) and abnormal (dishonest recommendations) over a span of time. We tested how a node trust value affects over a span of time with and without our proposed framework. Without any defence scheme, the nodes trust value would increase or decrease for some times and it is stable in the remaining time. With our scheme, the node trust value becomes stable as compared with CBRF. The better performance by proposed framework is due to maintaining the history of the recommendations made by remote assessing nodes on a particular assessed node 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 results are shown in Figure 8 and Figure 9.

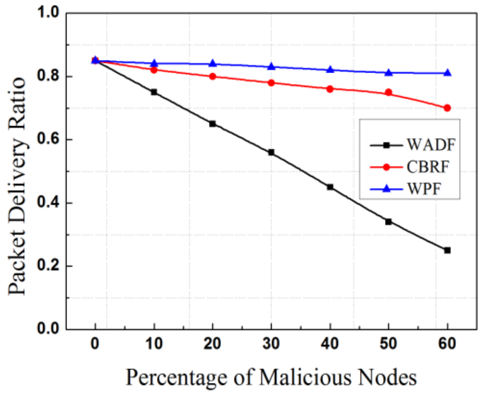

Figure.3 Malicious Nodes Vs Packet Delivery Ratio

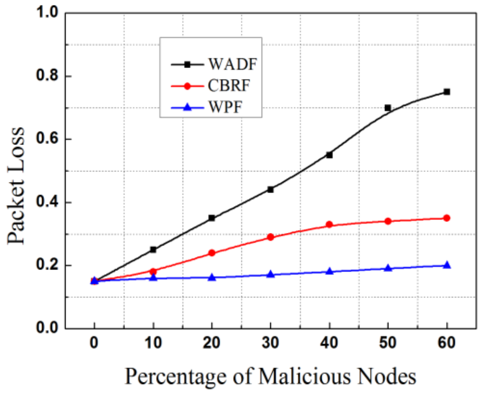

Figure.4 Malicious Nodes Vs Packet Loss

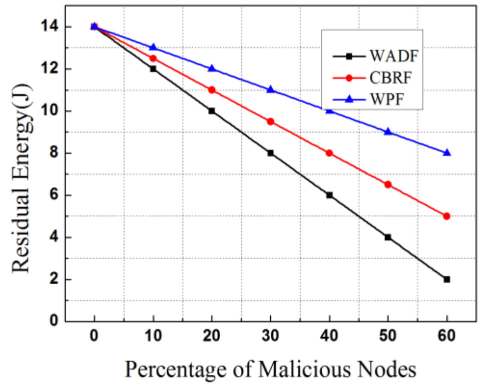

Figure.5 Malicious Nodes Vs Residual Energy

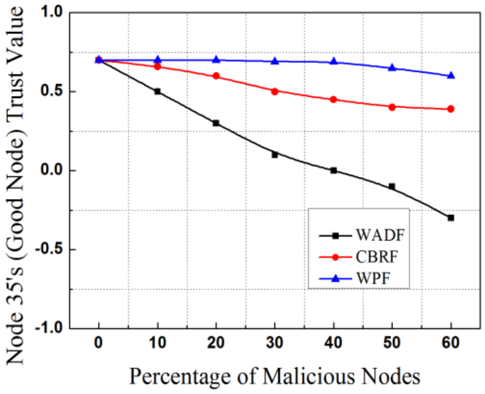

Figure.6 Malicious Nodes Vs Good Node Trust Value

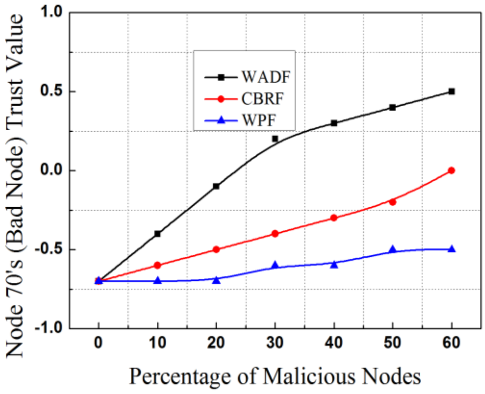

Figure.7 Malicious Nodes Vs Bad Node Trust Value

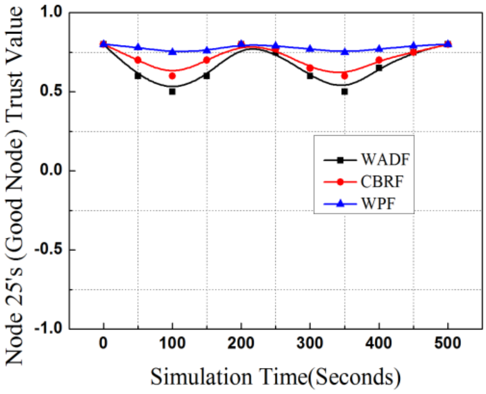

Figure.8 On-Off Attack on Good Node Trust Value

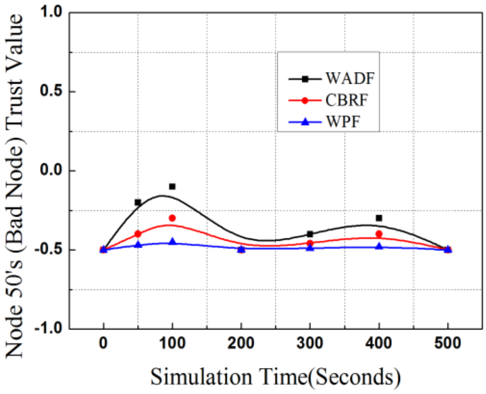

Figure.9 On-Off Attack on Bad Node Trust Value

5. Conclusion and Future Works

The significant attention paid from the research community on the concept of trust based group key management frameworks in terms of how to evaluate trust of nodes and use this information for various purposes. However, less work done in the context of attacks possible on the trust recommendations by malicious nodes in the network. Here, we proposed a framework based on three principles, namely threshold, average of recommendations and holding the history of recommendations. The Proposed framework is immune to the effect of trust values of nodes and performance of the network, even though in the presence of malicious or selfish behavior by up to 60% of nodes in the network. From these simulations, we conclude that the network performance significantly affects by malicious nodes and also our proposed scheme defends better compared with without any defence scheme and CBRF framework. Moreover, the results had shown the proposed framework can helpful in the context of MANETs. The other significant possible attacks on trust based frameworks are selective, position and seasonable attacks [6]. As part of future work, we are working on extending the proposed framework to mitigate these attacks also by assigning some weights to the recommendations based on location and time of the nodes on the network.

References

[1] Kamal Kumar Chauhan, Amit Kumar Singh Sanger, “Securing Mobile Ad hoc Networks: Key Management and Routing”, International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, pp.65-75, April 2012.

[2] Rafaeli S, Hutchison D, “A survey of key management for secure group communication”, ACM Computing Surveys, 35 (3), pp.309–329, 2003.

[3] Omar Cheikhrouhou, “Secure Group Communication in Wireless Sensor Networks: A survey”, Journal of Network and Computer Applications 61, pp.115-132, 2016.

[4] K. Cook, “Trust in society,” Russell Sage Found. Ser. Trust, vol. 2, no. 5, pp. 3–40, Feb. 2003.

[5] J.-H. Cho, A. Swami, and I.-R. Chen, “A survey on trust management for mobile ad hoc networks,” IEEE Commun. Surveys Tuts., vol. 13, no. 4, pp. 562–583, Nov. 2011.

[6] Zeinab Movahedi, Zahra Hosseini, Fahimeh Bayan, and Guy Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol. 18, No. 2, pp. 1287-1309, Second Quarter 2016.

[7] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, “Quantifying Trust in Mobile Ad-Hoc Networks,” Proc. Int’l Conf. Integration of Knowledge Intensive Multi-Agent Systems, pp. 65-70, April 2005.

[8] G. C. Hadjichristofi, W. J. Adams, and N. J. Davis, “A Framework for Key Management in a Mobile Ad Hoc Network,” Proc. Int’l Conf. on Information

Technology: Coding and Computing, Tiejun Huang, China, vol. 2, pp. 568-573, April 2005.

[9] 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, May 2006.

[10] B. J. Chang and S. L. Kuo, “Markov Chain Trust Model for Trust Value Analysis and Key Management in Distributed Multicast MANETs,” IEEE Trans. Veh. Technol., vol. 58, no. 4, pp. 1846-1863, May 2009.

[11] 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.

[12] G. Bella, G. Costantino, and S. Riccobene, “Managing reputation over MANETS,” in Proc. 4th Int. Conf. Inf. Assur. Security (IAS), pp. 255–260, 2008.

[13] Z. Movahedi, M. Nogueira, and G. Pujolle, “An autonomic knowledge monitoring scheme for trust management on mobile ad hoc networks,” in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), pp. 1898–1903, Apr. 2012.

[14] S. Almotiri and I. Awan, “Trust routing in MANET for securing DSR routing protocol,” PGNet, 2010.

[15] M. Seredynski and P. Bouvry, “Nature-inspired evaluation of data classes for trust management in MANETS,” in Proc. IEEE 26th Int. Parallel Distrib. Process. Symp. Workshops & PhD Forum, pp. 366–373, 2011.

[16] X. Li, M. R. Lyu, and J. Liu, “A trust model based routing protocol for secure ad hoc networks,” in Proc. IEEE Aerosp. Conf., vol. 2, pp. 1286–1295, Mar. 2004.

[17] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., pp. 90–100, 1977.

[18] 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. IEEE/ACM Int. Conf. Green Comput. Commun. (GREENCOM’11), pp. 124–130, 2011.

[19] Zhigang Li, Lingling Li, Fenfen Zhu, Quanming Zhao, "A New Algorithm of Closeness Degree for Fuzzy Pattern Recognition", International Journal of Intelligent Engineering and Systems, Vol.3, No.4, pp.9-16, 2010.

[20] W. Li, A. Joshi, and T. Finin, “Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach,” in Proc. 11th Int. Conf. Mobile Data Manage. (MDM’10), pp. 85–94, May 2010.

[21] 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, Dec. 2010.

[22] Y. Yuan, H. Chen, and M. Jia, “An optimized ad-hoc on-demand multipath distance vector (AOMDV) routing protocol,” in Proc. Asia-Pac. Conf. Commun., pp. 569–573, 2005.

[23] Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan 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.

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

[25] Thiruppathy Kesavan Venkatasamy, Radhakrishnan Shanmugasundaram, "Authentication in Wireless Sensor Networks Using Dynamic Keying Technique", International Journal of Intelligent Engineering and Systems, Vol.9, No.3, pp.146-155, 2016.

[26] X. Li, J. Slay, and S. Yu, “Evaluating trust in mobile ad hoc networks”, In: Proceedings of the Workshop of International Conference on Computational Intelligence and Security (CIS ’05), Springer, China, pp.1-10, 2005.

[27] Z. Liu, A. Joy, R.A. Thompson, “A dynamic trust model for mobile ad hoc networks”, In: Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS’04), pp.7-13, 2004.

[28] JH. Cho, A. Swami, IR. Chen, “A survey of trust management in mobile ad hoc networks”, IEEE Communications Surveys & Tutorials, Vol. 13, No. 4, Fourth Quarter, pp.562–583, 2011.

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

[30] Saravanan Nallusamy, Subramani Appavupillai, Sivakumar Ponnusamy, "Mobile Agents based Reliable and Energy Efficient Routing Protocol for MANET", International Journal of Intelligent Engineering and Systems, Vol.9, No.3, pp.110-117, 2016.