International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Reliable Group Key Management Framework Using Fuzzy Logic for MANETs

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

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

Abstract: Spontaneous group communication can be attained by deploying Mobile Ad Hoc Networks (or MANETs). The limitations 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. Trust value can be evaluated based on direct and indirect interactions with other nodes in the network. The threshold trust value does binary classification about a node is genuine or fake (misbehavior) and further communication includes or excludes. However, in many automated systems, the result for a given input cannot be just categorized as binary output. Instead of a binary, it is more spontaneous and natural to use a fuzzy set based classification which gives the degree of genuineness. To realize this concept, we propose a reliable group key management framework by adding fuzzy logic rules in this paper. The clustering scheme with Fuzzy classifier aids, to eliminate the pretended nodes over a span of time in order to evade internal attacks. Moreover, it saves the energy of each node due to lightweight framework and less key management overhead. Our simulation outcomes prove that our method is more reliable compared to existing frameworks.

Keywords: Reliability; Fuzzy Logic; Secure Group Communication; Group Key Management; Trust; Mobile Ad Hoc Networks.

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 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 Multicast Routing

Multicasting plays significant role in above collaborative applications of ad hoc wireless networks and boost the efficiency of the wireless nodes for communicating the same message to all intended group members at a time. The main reason to use a routing protocol with multicast capability is to decrease the process and control overhead, improve the efficiency by saving bandwidth, accept changes in topology and evades loops in the network, etc.

1.3 Role of Group Key Management

Group key also called as Traffic Encryption Key (TEK) management plays vital role in secure group communication systems and has two important modules called as security and efficiency [7]. 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.

1.4 Fuzzy Logic System

Fuzzy logic [23] can tolerate unreliable and imprecise inputs and takes decisions based on "degree of truth" rather than the traditional crisp logic values “true” or “false”. So it is used to handle the perception of partial truth values between “absolute truth” and “absolutely false”. For instance, the statement, Today is hot, might be 100% true if there are no clouds, 60% true if there is a little cloud, 40% true if it's cloudy and 0% true if it showers all day. Fuzzy logic has proven to be particularly useful to handle situations which were not defined precisely in automated artificial intelligence applications.

A typical Fuzzy logic system [28] has four key modules, namely Fuzzifier, Inference engine, Defuzzifier, and Rule Base as shown in Figure 1. Initially, a crisp set of input data is collected and transformed to a fuzzy set using fuzzy linguistic variables and fuzzy membership functions. This phase is called as fuzzification. Next, an inference is made based on a set of rules defined in the Rule Base. Finally, the resulting fuzzy output is mapped to a crisp output data using the membership functions, in the defuzzification phase. Linguistic variables are the input or output variables of the system whose values are non-numeric such as words or sentences of a natural language. For instance, Let Temperature (t) is the linguistic variable which represents the temperature of a room. To qualify the temperature, terms such as “hot" and “cold" are used in real life. These are the linguistic values of the temperature. We can represent like Temperature (t) = {too-cold, cold, warm, hot, too-hot}. A membership function is used to quantify a linguistic variable value and used in the fuzzification and defuzzification phases in order to map the non-fuzzy input values into fuzzy linguistic terms and vice versa. There are different forms of membership functions such as Triangular, Trapezoidal, Piecewise linear, Gaussian, Sigmoid, etc. The type of the membership function can be context dependent and it is generally chosen arbitrarily according to the user experience. A rule base is constructed to control the output variable. A fuzzy rule is a simple IF-THEN rule with a condition and a conclusion. For instance, if the temperature is cold and target is warm, then the command is heat. After the inference phase, the end result is a fuzzy value. This result should be defuzzified by defuzzifier component to obtain a final crisp output data. Defuzzification is performed according to the membership function of the output variable.

1.5 Problem Identification

Internal attackers are compromised nodes masking themselves as legitimate, honest members to disturb the system and it is difficult to differentiate between honest and dishonest nodes. A node can deny a service due to either less computing power in reality or with intention to disturb the system. Current group key management systems mostly focused on external attacks by incorporating authentication and integrity. However, any group key management technique without bearing in mind the internal attacks may not be useful. Some significant works also done to handle internal attacks and they proved that trust based group key management techniques are better than others.

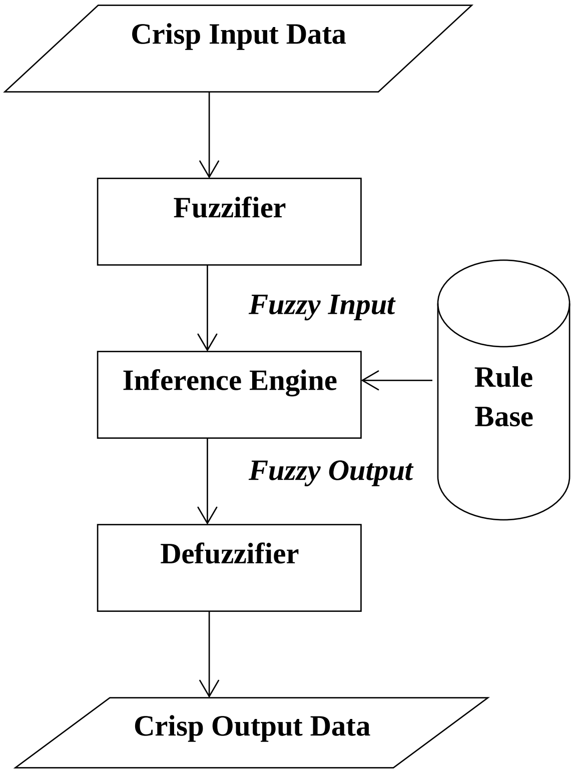

Figure.1 Working Model of a Fuzzy Logic System

Several approaches were proposed to evaluate the trust value for a node and the best one is the based on direct and indirect interactions of a node with other nodes. These techniques just do the binary classification for a node being either genuine or fake based on trust threshold value. For instance, in [0-1] scale, if the trust value of a node is more than 0.5 then it is genuine; otherwise it is fake.

However, in many automated systems, the result for a given input cannot be just categorized as binary output like either genuine (honest) or fake (dishonest) [9]. Instead of a binary, it is more spontaneous and natural to use a fuzzy set based classification which gives the degree of genuineness. Also, let the membership function of a fuzzy set can decide the tolerability of the genuineness of a node. To realize this concept, we propose a reliable group key management framework by adding fuzzy set rules in this paper. Here, build the conceptual model to the fuzziness to a trust value variable in the range of [-1, 1] where -1 represents node is absolutely fake and 1 represents node is absolutely genuine. Our experiments prove the reliability of fuzzy set based automated systems can improve than just binary classifier.

The contributions of this paper are as follows:

- Compared to current trust threshold-based group key management framework for MANETs, our intention is to provide a framework based on fuzzy-based classifier which can improve the reliability and stability of the system.
- Integrate the fuzzy classifier with clustering schemes for efficient key management.
- Eliminate the fake nodes over a span of time in order to handle internal attacks.
- The framework should be efficient, secure and reliable.

The remainder of the paper is structured as follows. In Section 2, we brief various group key management frameworks proposed so far for MANETs and the motivation for our proposal. We present an overview of the proposed framework in Section 3, and then, we provide the algorithm to eliminate dishonest nodes. In Section 4, we elucidate the implementation and results of our proposed framework and compare with existing significant works. Conclusion and future work remarks are in section 5.

2. Related Work and Motivation

Here, we brief existing group key management frameworks for SGC (Secure Group Communication) in MANETs and debate their pros and cons. In broad, we can say, flat-oriented (without organization of nodes) method and the virtual topology-oriented (with the organization) method. In the flat-oriented methods, without pre-organization of the nodes and straight away share a common group key (or TEK). In [11], the authors proposed CRTDH (Chinese Remainder Theorem and Diffie–Hellman) method for SGC. In this every node is participated to compute a TEK and then shared. However, it is not scalable due to dependence on all nodes. In [12], the authors proposed TRP (Two Round Protocol) where the originator of the protocol becomes the group Head and in first round sends a Hello message and in the second round computes the key. TRP needs little message overhead than CRTDH but hurts from a single point of failures. In [13], the authors proposed GKMPAN (probabilistic based) in which initially all nodes in the network are given some say n of keys out of a large set of m keys. The problem is, if any two nodes that do not have a group key need to use intermediate nodes. In [14], the authors proposed a two-stage secure and authentication protocol for multicast MANETs based on the trustworthiness of nodes. In this, they considered highest trustworthy node as group head, but didn’t describe the evaluation of trust values. In [15], the authors proposed key management based on static trust values, but it is not reliable in real time. In summary, the flat-oriented methods suffers from the single point of failure problem, where a single node message delay or join or leave affects all other nodes in the group. Also, they depend on a central server (group head) and so not scalable. In [27], the authors proposed a protocol based on mobile agents to save energy and increase reliability while routing. In [24], the authors proposed an authentication protocol for wireless sensor networks based on dynamic keying approach. However, it is not applicable straight away into a MANET environment in which frequent topology changes occurred due to node join or leave or moving around.

In the topology-oriented (Tree or Hierarchy based) group key management frameworks, the group nodes are virtually organized into hierarchical or tree topological structure. In fact, the topology-oriented methods put emphasis on improving key computation, message overhead and memory to store keys. However, these methods suffer from frequent topology changes due to node mobility or join or leave operations. In [16], a number of group key management protocols such as STR [17], CLIQUES [18] and TGDH [19] that was initially intended for local and wide-area wired networks have been revised to deal with the challenges of

MANETs. The revised protocols use Tree-based topology and ECC (Elliptic Curve Cryptography). The ECC benefits to the MANET environment in which nodes have limited computing power than public key cryptography because of the lesser key size and less computing overhead. However, these methods introduced fresh limitations like synchronization among nodes within the topology, especially when a node or link failure occurs. In [20], the authors proposed SGC Protocol based on the concept of clusters, where all nodes formed as set of clusters based on information maintaining about neighboring nodes. The information includes frequency of link failure, identity, degree, the residual power and the computation capability, etc. This information is to be used to form the cluster, elect a cluster head and further operations.

In [21], the authors proposed trust threshold-based ECGK (Efficient Clustering scheme for Group Key management) in which trust as a clustering criterion and used to distinguish between honest and dishonest group nodes. Their experiments proved that it is better suitable for MANET environment. However, it is based on threshold-based binary classification and also yet to deal with the rate of clustering while network in operation and dynamic change of trust relationships among nodes. In [22], the authors proposed CTPKM (Composite Trust-based Public Key Management) with a trust threshold design filter in order to handle untrustworthy messages or operations by attacker nodes. It can maximize availability and minimize vulnerability, without inviting more communication cost. However, their concept is also based on hard threshold-based node trustworthiness classification. For instance, say if trust value is more than 0.5 then it is genuine otherwise it is fake node. In most of the automated systems, it is better to use soft technique with degree of membership rather than hard technique with binary 0 and 1 value. This gives motivation to our work. In this work, we propose a soft computing based Reliable Group Key Management Framework, which uses Fuzzy Logic [or RGKMFFL] and compares with the existing hard trust threshold-based clustering schemes, ECGK and CTPKM. We show our proposed model outperforms than existing schemes in terms of efficiency, security and stability or reliability.

3. Proposed Framework

3.1 Overview

In this section, we elucidate our conceptual model to design the reliable framework based on Fuzzy set for group key management in MANETs. In this, we use the multicast feature in order to cope with bandwidth limitations. The trust value is evaluated for each node based on the direct and indirect observations. The mobility for each node also evaluated. The group members are clustered based on their wireless transmission range and the cluster head is picked out based on which node within the cluster has highest trust value and lowest mobility. The communication between nodes within the cluster will be direct and between the nodes which are in different clusters will be via Cluster Heads (CHs). In order to detect and eliminate misbehaving nodes, we use the fuzzy logic concept. Initially we treat every node is genuine based on the degree of trustworthiness and will give warning messages to the each node whose trust value is in below to the highest level so that it should improve the trustworthiness over a span of time from current level to the next higher level. Otherwise, it will be considered as fake node and it will be excluded from further communication.

3.2 Evaluation of trust for each node

The trust value for each node is evaluated based on the direct and indirect experiences [3] during the data transmission with other nodes in the cluster. The direct parameters such as correctness of packet delivery, obeying framework rules, packet correctness, involved in any attack such a black hole, selfish attack, etc., trust report by neighbors, rate of computing power drain are used to increase or decrease the trust value. Once the trust values collection over, the node assesses the trust value (TRUST (i, j)) with the following equation (1) [4].

$$\text{TRUST (i, j)} = \tanh\left(\sum_{w=1}^{n}\alpha_w\beta_w + \sum\nolimits_{w=1}^{m} TRUST(i,k) * TRUST(k,j)\right) \quad (1)$$

Where,
n - No.of of interactions between two nodes.
m - No.of nodes that sends the trust reports on node Nj to node Ni.
β_w - Weight of interaction number w.
α_w - +1, if interaction w is constructive.
α_w - -1, if interaction w is destructive.

The indirect interactions means if two nodes are not neighbors as illustrated in Figure 2. Let X and Y are the nodes are not within the transmission range. Let N_1, N_2… N_n be the one-hop neighbors. Node X can evaluate the trust value of node Y by considering the opinion from the common neighbor of both nodes. For this, we use Dempster -Shafer theory [6] which combines the degree of belief derived from the multiple common neighbors. Each common neighbor gives positive or negative opinion to node X based on the interaction with node Y.

3.3 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 (2) [5].

$$M_i^j = 10 \log 10 \frac{RSS_{i\to j}^{new}}{RSS_{i\to j}^{old}} \qquad (2)$$

Where,

$RSS - \beta * \vartheta * Ptx$ (3)

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

ϑ - The gain of the channel

Ptx = The transmitter signal power.

3.4 Formation of Clusters

To form a cluster, the procedure is as follows:

- The trust value for each node is evaluated as described in section (3.2) and the mobility is assessed as described in section (3.3)
- When the nodes are ready to deploy in the network, every node sends multicast Hello message to its neighboring nodes : Ni → Neighbouri: Hello
- After getting the Hello Message, each Ni finds itself and also identifies about its neighbors (L_{Neigh}).
- A node Ni declares itself as the CH, if it has highest trust and lowest mobility and updates this information by sending one more Hello message.
- Now all neighboring nodes join with corresponding CH and form the cluster.
- 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.

The Figure 3 illustrates the formation of cluster mechanism. It includes three clusters C_1, C_2 and C_3. N_3, N_7, and N_{11} are chosen as cluster Heads CH_1, CH_2, and CH_3 respectively because of their own highest trust value and lowest mobility.

3.5 Group Key Management

The common group key will be compute by using CRTDH [11]. Here, group key is computed as a function of share provided by altogether in the cluster. This technique needs two rounds of multicasts to establish the TEK. In the first round, the Cluster Head initiates the computation and collects a share of each member. In the second round, the Cluster Head computes the TEK and then broadcasts it to all members. In order to guarantee backward and forward secrecy the group key should be updated on every occurrence of an old member leaves from the group or a new member joins in the group or any topological changes due to mobility.

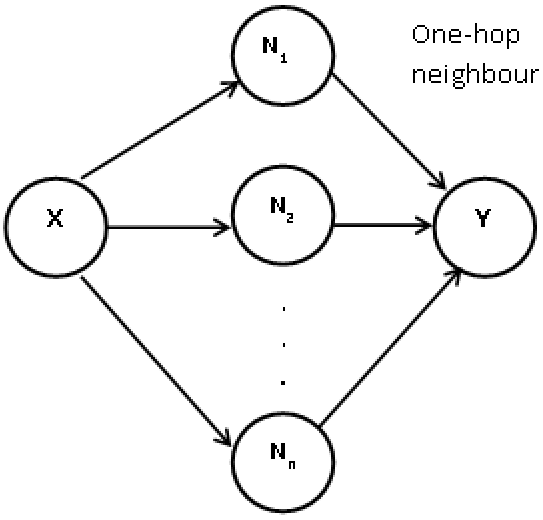

Figure.2 System model to evaluate indirect trust

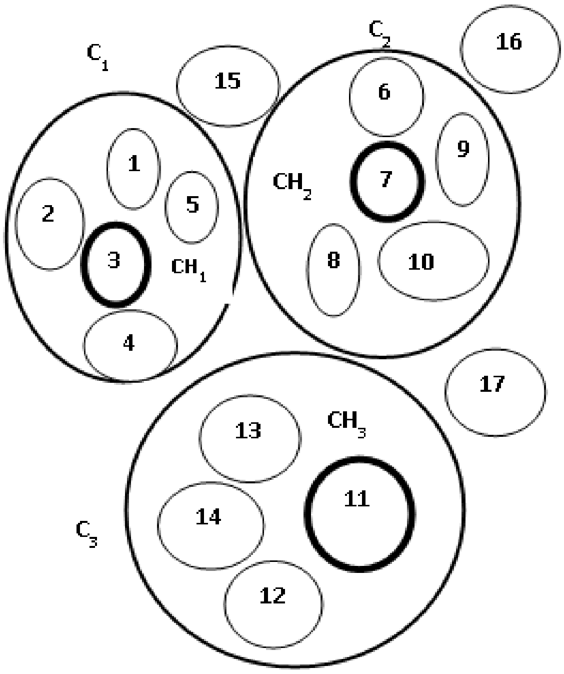

Figure.3 Formation of Clusters

3.6 Dealing Dishonest Nodes by Fuzzy Logic

To distinguish between honest and dishonest nodes, we need to take into account about trust relations in addition to authorization. In other words, we need a mechanism to handle insider or internal attacks posed by pretending nodes. In existing cluster based frameworks, ECGK and CTPKM, just done the binary classification based on the trust threshold value (for instance, say 0.5) in order to decide a node is genuine or malicious. In our work, we propose a soft computing technique named as Fuzzy logic based procedure is used to separate dishonest nodes from honest nodes by incorporating fuzzy logic rules based on trust value. We use fuzzy set membership function which describes the degree of genuineness about node trustworthiness. As per the discussion in section 1.4, the fuzzy set membership function and Rule base are defined in the Table 1 and Table 2 respectively. We considered two linguistic variables, namely Trustworthiness and Eliminate_Risk. So we can write Trustworthiness (Node) = {Excellent, Very Good, Good, Fair, Poor} and Eliminate_Risk (Node) = {NIL, Low, Moderate, High, Very High}. We elected sigmoidal membership function, *sigmf (x, [a c]),* as given in the following equation (4) by *f (x, a, c)* is a mapping on a vector x, and depends on the parameters a and c.

$$f(x,a,c) = \frac{1}{1+e^{-a(x-c)}} \qquad (4)$$

The sigmoidal membership function is inherently open to the right or to the left based on sign of parameter a, and thus is appropriate for representing concepts such as "very positive" or "very negative." Also, it is suitable in order to handle asymmetry of trust crisp input data between [-1, 1].

Table 1. Fuzzy Set Membership Function

Trust value of a node	Trustworthiness of a node	Eliminate 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

Table 2. Fuzzy Rule Base for Proposed System

Fuzzy Rules
• **IF** (Trustworthiness(N_i) is *Excellent*) **THEN** Eliminate_Risk(N_i) is *NIL* • **IF** (Trustworthiness(N_i) is *Very Good*) **THEN** Eliminate_Risk(N_i) is *Low* • **IF** (Trustworthiness(N_i) is *Good*) **THEN** Eliminate_Risk(N_i) is *Moderate* • **IF** (Trustworthiness(N_i) is *Fair*) **THEN** Eliminate_Risk(N_i) is *High* • **IF** (Trustworthiness(N_i) is *Poor*) **THEN** Eliminate_Risk(N_i) is *Very High*

3.7 Working Model of Proposed System

The flowchart in Figure 4 describes about the working model of our proposed system using a fuzzy logic system with Rule base (i.e. IF-THEN control structures) to eliminate dishonest nodes from the network to avoid further communication with those nodes. To detect and eliminate the dishonest nodes over a span of time, we assumed that initially each node is genuine and later broadcast a warning/cautious message to the nodes which are under elimination risk such as Low, Moderate, High and Very High. The alert message consists of warning to each such node so that you are in risk mode and improve your performance over a span of time otherwise you may be eliminated from the network. Though after receiving cautioning messages, if some nodes unable to downgrade its eliminate risk level over a span of time, then these will be treated as dishonest nodes and eliminated from the network.

4. Results

4.1 Simulation Configurations

To simulate our proposed RGKMFFL framework, we used NS2 [10] tool. We conducted four experiments with varying number of dishonest or attacker nodes from 0 to 10. The Constant Bit Rate (CBR) type of data packets used here. The area size is 1000 meter x 1000 meter square region for a simulation time of 500 seconds. We evaluate and compare the performance of our framework RGKMFFL with the ECGK [21] and CTPKM [22] by considering the performance metrics [8] Packet Delivery Ratio, Residual Energy, Packet Loss Ratio, and number of controlling packets for Key

Management (Overhead) by varying the number of attackers over a span of time. Our simulation settings with key parameters are listed in Table 3.

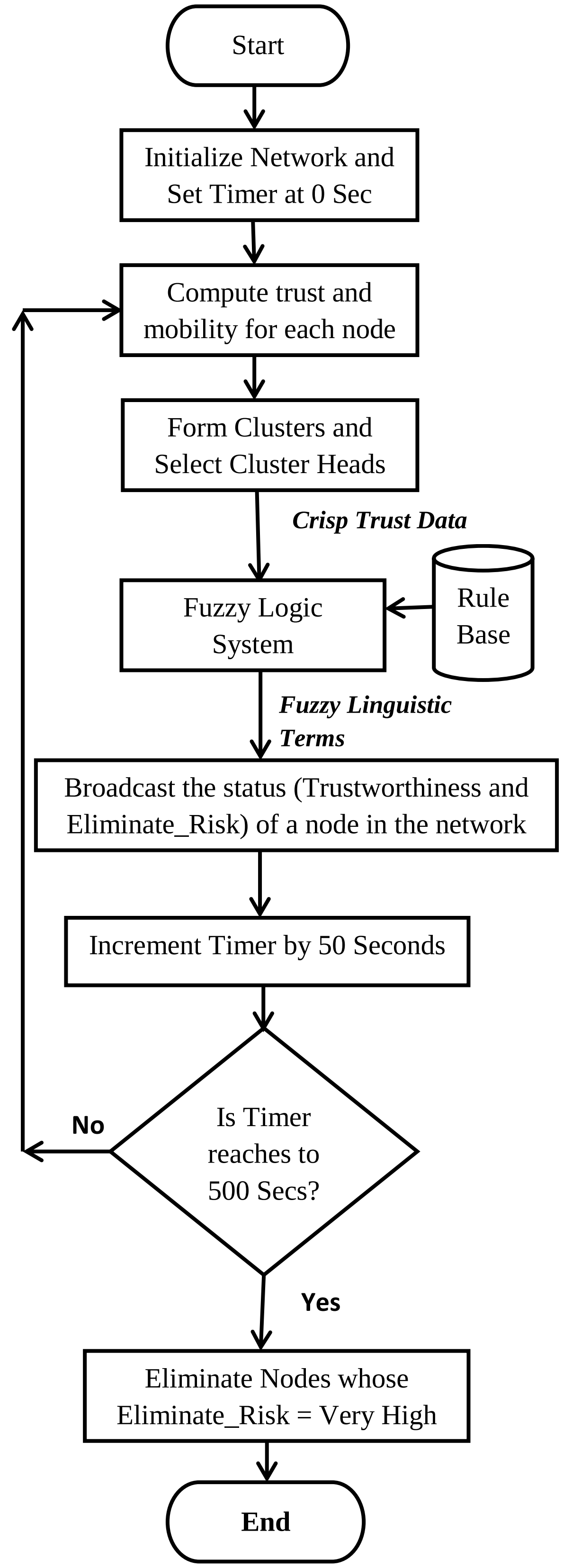
Start
Initialize Network and Set Timer at 0 Sec
Compute trust and mobility for each node
Form Clusters and Select Cluster Heads
Crisp Trust Data
Fuzzy Logic System
Rule Base
Fuzzy Linguistic Terms
Broadcast the status (Trustworthiness and Eliminate_Risk) of a node in the network
Increment Timer by 50 Seconds
Is Timer reaches to 500 Secs?
No
Yes
Eliminate Nodes whose Eliminate_Risk = Very High
End

Figure.4 The working model of proposed framework

Table 3. Simulation settings

Number of Nodes	50
Area	1000 X 1000
MAC	802.11
Simulation Time	500 Sec
Traffic Source	CBR
Number of Attackers	Between 0 and 10
Antenna	Omni Antenna
Pause Time	100 m/s
Initial Energy	15 J
Transmission Power	0.770
Receiving Power	0.425
Propagation	Two-ray ground reflection model

4.2 Results Analysis

For each performance metric, a separate experiment was conducted by varying the number of attackers over a span of simulation time 500 Sec. The results for three frameworks are plotted in the below Figures 5 to 8. By seeing the results of these three frameworks, we infer that RGKMFFL beats ECGK and CTPKM by 20% improved with respect to Packet Delivery Ratio, 22% reduced with respect to Packet Loss Ratio, 10% increased with respect to Residual Energy and 25% reduced with respect to Key Management Overhead. Even though the number of attackers increased, our framework performance is better due to the initial misbehaved nodes can set right because of cautionary messages about the elimination risk.

5. Conclusion and Future Works

In this paper, we proposed a reliable, efficient and secure group key management framework for MANETs. In this framework, a lightweight fuzzy rule set is used to improve efficiency and eliminate the dishonest or attacker nodes over a span of time. Here trust value is determined for each node based on the direct and indirect observations.

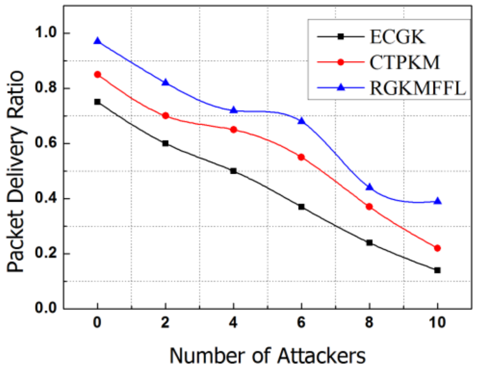

Figure.5 Attackers Vs Packet Delivery Ratio

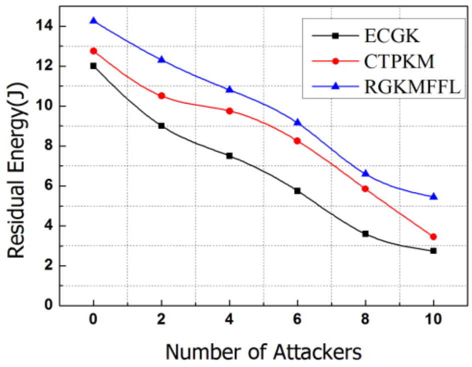

Figure.6 Attackers Vs Residual Energy

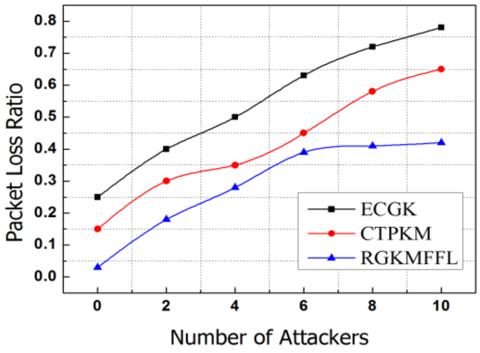

Figure.7 Attackers Vs Packet Drop

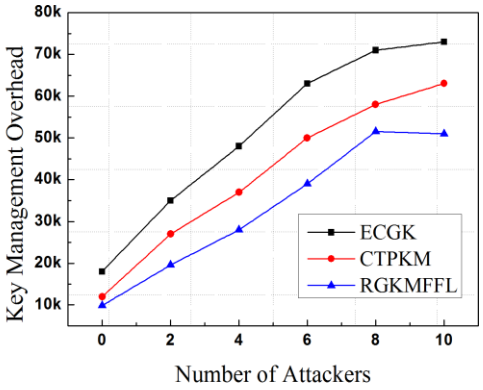

Figure.8 Attackers Vs Key Management Overhead

The network is clustered and the cluster head is elected based on the highest trust vale and lowest mobility. The procedure for group key management and handle the attackers described. By simulation results, we proved that the proposed technique reduces the complexity and overhead and so leads to save computing power of each node. A weakness of using fuzzy logic is that storing the rules database might involve a significant amount of memory. As a future work direction, we plan to investigate defence mechanisms for attacks such as bad-mouthing, ballot-stuffing, and collusion [25] [26] posed by dishonest nodes.

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] 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.

[4] 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.

[5] 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.

[6] L. Zadeh, “A simple view of the Dempster-Shafer Theory of Evidence and its implication for the rule of combination”, The Al Magazine, Vol. 7, No. 2, pp.85-90, 1986.

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

[8] Reham Abdellatif Abouhogail, “Security Assessment for Key Management in Mobile Ad Hoc Networks”, International Journal of Security and Its Applications, Vol.8, No.1, pp.169-182, 2014.

[9] F.B. Bastani, I-R. Chen, T. Tsao, “Reliability of systems with fuzzy-failure criterion”, in Annual Reliability and Maintainability Symposium, Anaheim, CA, pp.442–448, 1994.

[10] Network Simulator NS2 available online: http://www.isi.edu/nsnam/ns.

[11] R.K. Balachandran, B. Ramamurthy, Z. Xukai, N.V. Vinodchandran, “CRTDH: an efficient key agreement scheme for secure group communications in wireless ad hoc networks”, In: IEEE International Conference on Communications, (ICC 2005), vol. 2, pp.1123–1127, May 2005.

[12] R. Bhaskar, D. Augot, V. Issarny, D. Sacchetti, “An efficient group key agreement protocol for ad hoc networks”, In: IEEE Workshop on Trust, Security and Privacy in Ubiquitous Computing, Taormina, Italy, pp.12–16, June 2005.

[13] S. Zhu, S. Setia, S. Xu, S. Jajodia, “GKMPAN, An efficient group rekeying scheme for secure multicast in ad-hoc networks”, In: MobiQuitous, IEEE Computer Society, pp.42–51, 2004.

[14] L. Xu, X. Wang, J. Shen, “Strategy and simulation of trust cluster based key management protocol for ad hoc networks”, In: 4th Inter- national Conference on Computer Science and Education, Nanning, China, pp.269–274, 2009.

[15] BJ. Chang, SL. Kuo, “Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs”, IEEE Transactions on Vehicular Technology, 58 (4), pp.1846–1863, 2009.

[16] M. Manulis, “Contributory group key agreement protocols, revisited for mobile ad-hoc groups”, In: Proc. of the 2nd IEEE Int’l Conference on Mobile Sensor Systems, MASS’05, IEEE Computer Society, pp.811–818, 2005.

[17] Y. Kim, A. Perrig, G. Tsudik, “Group key agreement efficient in communication”, IEEE Transactions on Computers 53 (7), pp.905–921, 2004

[18] M. Steiner, G. Tsudik, M. Waidner, “Key agreement in dynamic peer groups”, IEEE Transactions on Parallel and Distributed Systems, 11 (8), pp.769–779, 2000.

[19] Y. Kim, A. Perrig, G. Tsudik, “Tree-based group key agreement”, ACM Transactions on Information System Security, 7 (1), pp.60–96, 2004.

[20] Y-M. Tseng, C-C. Yang, D-R. Liao, “A secure group communication protocol for ad hoc wireless networks”, Advances in Wireless Ad Hoc and Sensor Networks, Signals and Communication Technology Series, Springer, pp.102-130, 2007.

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

[22] J. Cho, I. Chen, K. S. Chan, “Trust threshold based public key management in mobile ad hoc networks”, Ad Hoc Networks 44, pp.58–75, 2016.

[23] Z. Li, L. Li, F. Zhu, Q. 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.

[24] T. K. Venkatasamy, R. 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.

[25] 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, NO. 2, SECOND QUARTER, pp.1287-1309, 2016.

[26] 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, OCTOBER, pp.2101-2155, 2015.

[27] S. Nallusamy, S. Appavupillai, S. 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.

[28] J. Mendel, “Fuzzy logic systems for engineering: a tutorial”, Proceedings of the IEEE, 83 (3), pp.345-377, Mar 1995.