TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 6140 - 6158

An Adaptive Fuzzy System based Insider Attacks detection with Group Key management for Wireless Ad-Hoc Network

[1*]C. Sivakumar Chellappan, [2]Dr .C. Nalini
[1*]*Research scholar, Computer Science and Engineering, BIHER*
[2]*Professor, Computer Science and Engineering, BIHER*
[1*]*Email:sivakumart.itcareer@gmail.com*

Article Info
Volume 81
Page Number: 6140 - 6158
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *28 December 2019*

Abstract:
Ad-hoc networking of wireless devices permits the establishment of contact links on the taking part hubs without pre-arranged infrastructure. In wireless ad hoc networks, participatory nodes typically engage in group communications such as broadcast, multi-access or relay functions. Protecting these communications is a challenging task, as internal attackers may secretly cause damage to the network, which is difficult to predict. Internal attackers can affect the sensors negatively and may disrupt the network by dropping sensitive packets or modifying packet information maliciously. Inside attackers are capable of causing many types of activities as well as passive attacks. Attackers located at a critical point in the network can significantly affect network performance. Insider attackers conceal themselves by marking themselves as legitimate nodes. Therefore it becomes hard for the system to differentiate dishonest nodes from honest nodes. So as to make the communication among the network more secure, an adaptive fuzzy system that uses CSO algorithm for selecting optimal membership function has been proposed. In this approach, the group key is distributed by the cluster head to the cluster members. This makes sure that only the nodes with the same group key can speak with one another. Implementing appropriate group-key management in the system that focuses on internal attacks identifies the dishonest nodes which can be then eliminated through some other security measures. This ensures the absence of the dishonest nodes inside the network. The results have been simulated and the execution of the proposed approach has been contrasted with the tradition FS approach. The results have shown the presented approach has performed better than the traditional approach.

Keywords: *Adaptive Fuzzy System, Cat Swarm Optimization, Group key management, Wireless Ad-hoc Network, Insider attack, Membership function.*

1. Introduction

Wireless networks can be arranged in two sorts: - foundation network and framework less (ad hoc) networks. Framework less network is known as a wireless ad hoc network (WANET). WANET can be confined by a self-administering plan of hubs that are related wirelessly without requiring any foundation or focal authority [1, 2]. The advantages of wireless networks are Independence from focal network administration, Self-designing, hubs are likewise switches, adaptability is like having the option to get to the web from a wide range of areas and versatility. Insider dangers are characterized as cybersecurity dangers that originate from inside your own organization [3].It might be a worker or a merchant – even ex-representatives. Anybody that has legitimate access to your network can be an insider risk [4]. This assault dependent on the use of the data, e.g., keying material, put away on the traded off sensor hub. This empowers the adversary to show up as a genuine hub in the network. This contrasts from the old-style see, where an inside adversary might be an individual with a broad learning of and favored access to the objective framework and can assault inside a frameworks' border resistance, e.g., a previous representative of an organization. A few assaults can be found in an insider assault [5, 6].

They are undermined representatives or merchants, indiscreet workers' and the malignant insider. These dangers are utilized in WANET [7]. As of late, a few strategies are utilized to identify the insider assault in WANET. Along these lines, adaptive fluffy frameworks are utilized [8]. Adaptive fluffy is utilized to identify and dispensing with hubs in an insider assault in the network. To improve the proposed fluffy framework, Chemical Reaction Optimization (CRO) calculation is utilized to locate the ideal enrollment capacities. The exhibition of the proposed methodology is assessed regarding bundle conveyance proportion, parcel misfortune rate, vitality effectiveness and network lifetime [9, 10].

2. Literature Review

Wang, N. C., *et al.* [11] was broke down a Space Division Multiple Access (SDMA) -based MAC convention for WANET with shrewd receiving wires. The proposed convention abuses the SDMA framework to permit the gathering of multiple bundles from spatially isolated transmitters. Utilizing SDMA innovation gives crash-access is free to the correspondence medium dependent on the area of a hub. Recreation results show the adequacy of the proposed S-MAC in developing throughput and expanding spatial channel reuse. This convention doesn't accept any information on the area of neighboring hubs has the principle impediment.

Weakly Connected Dominating Set(WCDS) - helped insect-based steering convention for WANET was created by Li, K. H., *et al*. [12]. This paper utilized the grouping idea of WCDS to propose adeveloped Ant-dependent on interest Clustering Routing (AOCR) convention for WANET. Network states' data was gotten from the Forward Ant and just communicate by the head of each group, in this way diminishing the overhead required to transmit insect bundles. To build network proficiency, the pseudo-irregular relative choice procedure was utilized to assess the best way from the source hub to the goal hub by the Reverse Ant.

Logical Key Hierarchy Plus(LKH++) based Group Key Management plan for Wireless Sensor Network was created by Yao, W., *et al.* [13]. This paper proposed a safe low-control gathering key administration plan dependent on LKH. In our plan, we build a safe tree to oversee gathering keys. The structure technique for key tree and holding method for keys were proposed by our plan to decrease calculation and capacity overhead on every sensor hub. In addition, Wireless Logical Key Hierarchy (WLKH) bolsters rekeying to upgrade organize security and survival against hub catch. Execution investigation demonstrates WLKH is exceptionally effective as far as security, calculation, and key stockpiling.

A Bayesian deduction based discovery instrument to shield restorative cell phone networks against insider assaults was created by Meng, W., *et al*. [14]. In this paper, we centre on MSNs and present a conservative however productive Faith-based methodology utilizing Bayesian deduction to distinguish malevolent hubs in such a domain. We at that point exhibit the adequacy of our methodology in recognizing malignant hubs by assessing the sending of our proposed methodology in a genuine situation with two human services associations.

Meng, W., *et al.* [15] examined identifying insider assaults in therapeutic digital-physical networks dependent on social profiling. The identification of pernicious gadgets in Medical Smartphone Networks (MSNs) and structure a trust-put together recognition based with respect to social profiling. A hub's notoriety can be made a decision by recognizing the distinction in Euclidean separation between two conduct profiles. In the assessment, we assess a genuine MSN condition by teaming up with a commonsense social insurance focus. The test result showed that can recognize noxious MSN hubs quicker than other comparative approaches.

Vitality proficient fluffy adaptive determination of confirmation hubs in wireless sensor networks was created by Akram, M., *et al*. [16]. We proposed a Fuzzy-based versatile choice of the middle check hubs in PVFS to accomplish ideal vitality reserve funds. We show that our proposed technique accomplishes better vitality preservation within the sight of both the previously mentioned security dangers while giving a similar high sifting control of the PVFS.

A Power-efficient Adaptive- Fuzzy Resolution Control System for Wireless Insufficient Sensor Networks dissected by Chen, S. L. *et al*. [17]. In this paper, a medium-power and big-calibre adaptive fluffy goals power framework were made for wireless body sensor networks. The goals of the recognized sign can be adaptively changed by the quick element of the sign. The proposed adaptive fluffy goals controller acknowledged by VLSI execution. It can work at 100 MHz with just 539 door tallies, and it was centre zone is 7124 μm^2, orchestrated utilizing a 0.18-μm CMOS process. The outcome demonstrated that just improve the nature of the ECG flag in an unusual locale yet in addition decrease transmission control for wireless body sensor networks.

3. Proposed methodology:

Most existing group key management approaches are focused on external attacks only. This makes the system more powerful against external attacks but makes it vulnerable to internal attacks. Dishonest nodes that act as straight nodes need to be identified so that they can be rectified or eliminated. For this purpose,in this work, a new approach is proposed. First, the trust values and mobility of each node in the network are evaluated. Based on these trust values and mobility, the leader of a cluster is elected. The selected cluster head then produces the gathering key and disseminates the gathering key to the gathering members. Only nodes with the same group key can communicate with each other. This ensures security on the network. To further improve security, the proposed adaptive fuzzy system eliminates malicious nodes and insider attacks on the network. The Cat Swarm Optimization (CSO) algorithm is used to find the optimal membership functions.

3.1.Trust-based evaluation:

The trust value is calculated for each node, depending on direct and indirect encounters during information transmission with different hubs in the cluster. For increasing and decreasing the trust value, some direct parameters, such as packet correctness, obeying framework rules, packet delivery, involved in any attack like a selfish attack, black hole assault, etc., trust list by neighbors, rate of processing power drain isutilized. When the collection of trust values is complete, the node evaluates the trust value.

$$T(h,i) = \tanh\left(\sum_{v=1}^{m} \alpha_v \beta_v + \sum_{v=1}^{l} T(h,j) * T(j,i)\right) \tag{1}$$

Where m represents the quantity of interactions between two nodes, l represents the number of hubs that transmits the trust report on hub N_i to N_h, β_v denotes the weight of the interaction number v. α_v represents the constructiveness and destructiveness of the interaction v. α_v is +1 when the interaction v is constructive and α_v is -1 when the interaction v is destructive. The interaction is said to be indirect when the nodes are not neighbours and needed to interact with each other.

3.2.Node mobility calculation:

By computing the ratio of Received Signal Strength (RSS) among the two progressive information transmissions from a neighbour node, the mobility for every node i with respect to node h (L_h^i) can be defined in equation (2).

$$L_h^i = 10\log 10^{\frac{RSS_{h->i}^{new}}{RSS_{h->i}^{old}}} \tag{2}$$

Here,

$$RSS = \beta * \vartheta * TSP \tag{3}$$

Where,

β is constant that relies on the antennas and the wavelength ϑ is the gain of the channel and TSP is the transmitter signal power.

3.3.Cluster formation:

For each node, the trust value is evaluated, and their mobility is assessed. When the nodes are ready to deploy, all nodes send a multicast hello message to their neighboring nodes (Nh). All the Nhs find themselves and identify their neighbors (Kneigh). When a node has very low mobility and high trust value, the node declares itself to be the cluster head and then refreshes this data by sending another welcome message. After this, the neighboringhubs form the cluster together with the corresponding cluster head. When there are some nodes that do not join the cluster and hold the trust relation with at minimum one cluster, then they join the cluster with the most extreme trust value.

3.4.Group key management:

Because of the requirement of security,scalability under the restrictions of nodes' available resources and unpredictable mobility the large and dynamic groups' group key management becomes a difficult problem. The group key management protocols that are specifically designed to function in wired networks are not compatible with MANET due to the attributes and the difficulties of such environments.

3.5.Fuzzy system:

Designers utilize fuzzy rationale to create complex control frameworks are discovering support from a related technology. By remembering adaptive control for their game plans, they can structure frameworks that can acclimate to natural changes in wide applications. These adaptive frameworks get their capacity from, from one viewpoint, their ability to learn and clarify their thinking and, on the other, from their ability to be altered and expanded. Finding some kind of harmony between learned responsiveness and unequivocal human information makes the frameworks strong, extensible, and appropriate for taking care of an assortment of issues. Ongoing uses incorporate demonstrating of econometric changes, assessing organizations for conceivable obtaining, test-promoting new items, and mapping key field powers in reproduced war games. On the other hand, conventional fuzzy rationale frameworks, as regular proportional-integral-derivative (PID) control frameworks, can't adjust to slow changes in their surroundings. They can, obviously, modify their conduct starting with one execution of the guidelines then onto the next, yet the standards themselves don't change. Static frameworks of this sort are fine for applications in which the earth is known and unsurprising. Be that as it may, they can prompt catastrophe when the presumptions whereupon they are fabricated are abused. A conventional fuzzy framework standardizes and changes over the contributions to fuzzy form, executes the guidelines important to the information sources, and defuzzifies the resultant yield fuzzy sets. It can alter its conduct during an execution cycle in the light of the outcomes of a past cycle, yet it doesn't redesign itself or modify its guidelines to suit changes in its condition.

3.6.Adaptive fuzzy system:

An adaptive fuzzy rationale framework not just acclimates to time or process-phased conditions, yet additionally changes the supporting framework controls. This means an adaptive framework changes the attributes of the guidelines the topology of the fuzzy sets, and the technique for defuzzification dependent on prescient intermingling measurements. In the manner they work, versatile fuzzy systems look like neural systems. Fuzzy systems display conduct that compares to that of a neural framework at its root level. The two frameworks are prepared through an exhibition metric, typically a lot of cases demonstrating info and an ideal yield; and both go about as classifiers, and where the characterization space is escalated by changes to loads that are balanced by how much the framework is in error. An adaptive fuzzy framework, nonetheless, is substantially more advanced and has a higher degree of adaptive parameters. Such frameworks are likewise better ready to manage their human accomplices since they can, basically, clarify their reasoning.

Trust relation and authorization are taken into account to distinguish Honest node and dishonest. This is useful for dealing with internal or insider attacks. In the existing approaches, to find the honest and dishonest node, the trust threshold value based binary classification has been performed. A soft computing technique known as an adaptive fuzzy system is presented in the proposed approach for separating honest nodes from the dishonest node. The proposed adaptive fuzzy system incorporates trust value-based fuzzy logic rules. The fuzzy set participation work shows the degree of genuineness about node trustworthiness. Two linguistic variables such as trustworthiness and elimination risk are considered as membership function in the proposed approach. The parameters in trustworthiness of node are Excellent, very good, good, fair and poor. The parameters in eliminate risk of node are NIL, low; moderate, high, exceptionally high. Both the trustworthiness and eliminate risk of a node are inversely proportional to each other. When the trustworthiness is excellent, the eliminate_risk is NIL. The eliminate_risk is low when the trustworthiness is very good. When the trustworthiness is good, the eliminate_risk is moderate. The eliminate_risk is high when the trustworthiness is fair. When the trustworthiness is poor, the eliminate_risk is very high. In the proposed approach, the fuzzy logic system with Rule base is used for eliminating dishonest nodes from the honest nodes in the network. After eliminating the dishonest nodes, further communication with these nodes are avoided. In order detect and remove unreliable nodes over a period of time, an assumption is made that all nodes are initially true, and then a warning or warning message is broadcasted to nodes that are in low, moderate, high, and very high risk of elimination. The warning to every such node is contained in the alert message so that the respective nodes can know that they are under the risk of elimination and they can improve their performance over the period of time. If some hubs are unfit to minimize their elimination risk over the given period of time even after receiving the warning message, then those nodes are considered as the dishonest nodes and they are eliminated from the network. Table 1 shows the fuzzy set membership function and Table 2 shows the fuzzy guidelinebase for proposed framework. Figure 1 exhibitthe functioning model of fuzzy in the proposed system.

Table 1: Fuzzy set membership function

Trust value	Trustworthiness	Eliminate risk
0.5 to 1	Excellent	NIL
0 to 0.49	Very Good	Low
-0.3 to -0.01	Good	Moderate
-0.6 to -0.31	Fair	High
-1 to -0.61	Poor	Very High

Table 2: Fuzzy rule base for the proposed system

Fuzzy Rules

IF Trustworthiness is Excellent
Then Eliminate_Risk is NIL
IF Trustworthiness is very Good
Then Eliminate_Risk is Low
IF Trustworthiness is Good
Then Eliminate_Risk is Moderate
IF Trustworthiness is Fair
Then Eliminate_Risk is High
IF Trustworthiness is Poor
Then Eliminate_Risk is Very High

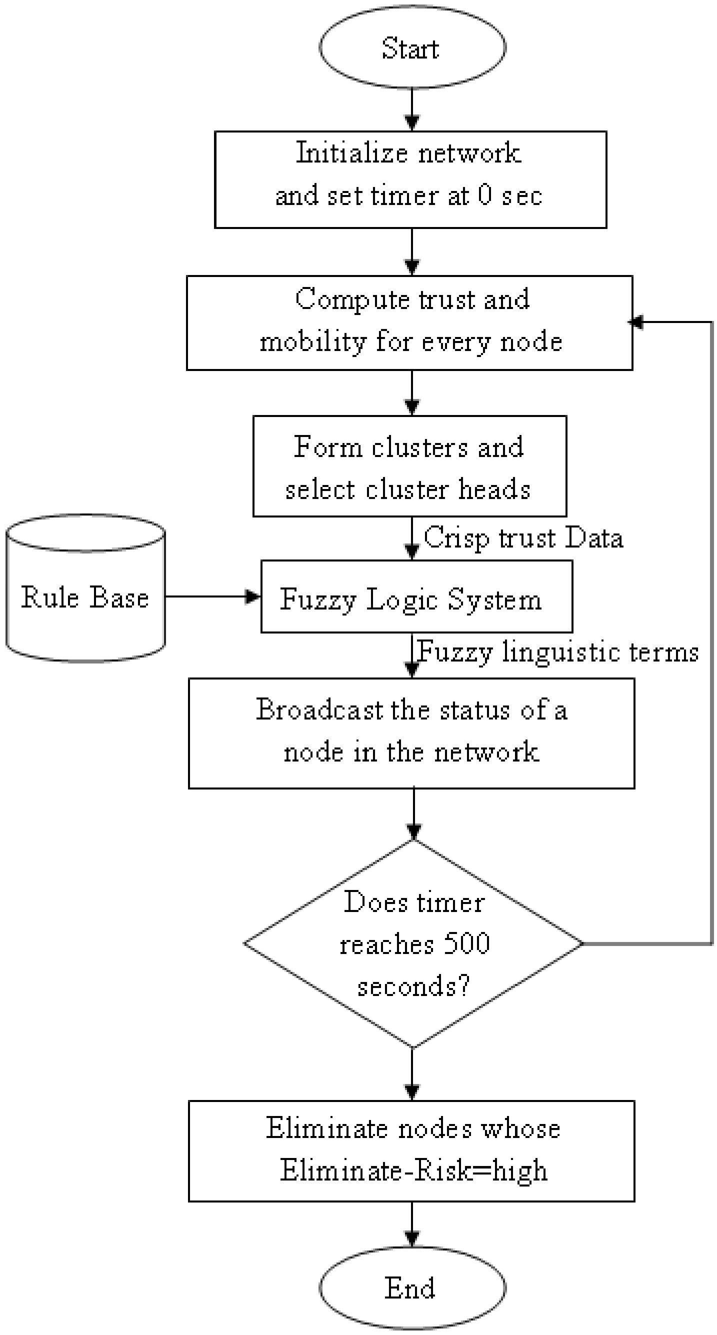
Start
Initialize network and set timer at 0 sec
Compute trust and mobility for every node
Form clusters and select cluster heads
Crisp trust Data
Rule Base
Fuzzy Logic System
Fuzzy linguistic terms
Broadcast the status of a node in the network
Does timer reaches 500 seconds?
Eliminate nodes whose Eliminate-Risk=high
End

Figure 1: The working model of fuzzy in the proposed system

Fuzzification: Input crisp values of Trustworthiness (TW) and Eliminate_Risk (ER) are converted into variablesfuzzy. Then the membership work is determined for every fuzzy variable. The yield parameter of the proposed method is the Trust score. For TW, variables fuzzy are classified in the range [-1, 1] and are classified as Excellent, Very Good, Good, Fair and Poor. For TW, variables fuzzy are classified in the range [-1, 1] and are classified as NIL, Low, Moderate, High and Very High. For obtaining the optimum outcomes, triangularand trapezoidal membership functions are utilized in this model. These trapezoidal and triangular membership functions are used for a boundary and intermediate variables. Input variables fuzzy Variables membershipfunction TW and

ER are shown in Figure 2 and Figure 3 respectively.

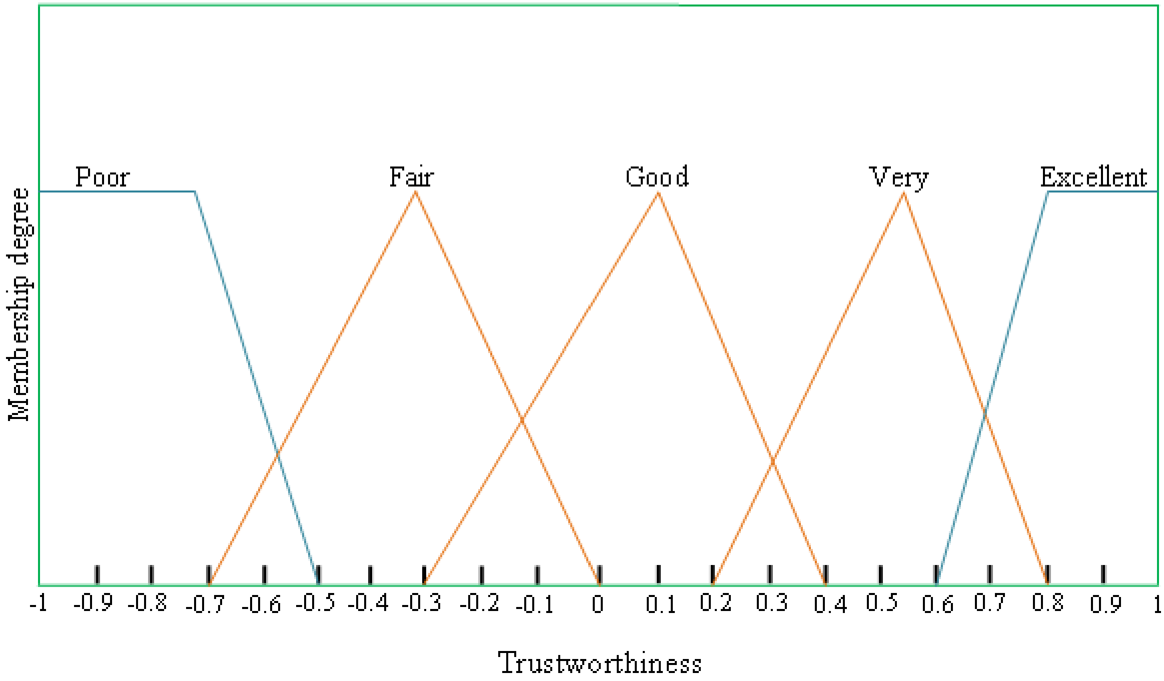

Figure 2: Membership function of TW

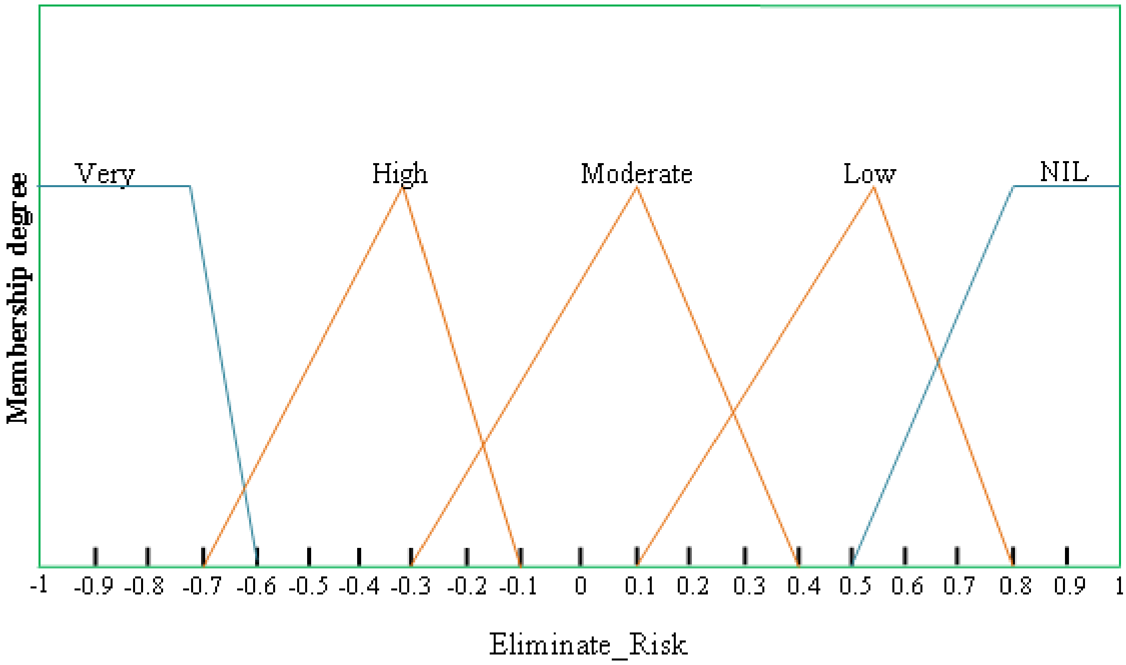

Figure 3: Membership function of ER

Defuzzification:Defuzzification is the way toward creating a quantifiable outcome in Crisp logic, given fuzzy sets and relating enrollment degrees. The procedure maps a fuzzy set to a crisp set. It is commonly required in fuzzy control frameworks. The fuzzy rule base is shown in Table 3.

Table 3: Fuzzy rule base

Rule No	TW	ER	O/P
R1	Excellent	NIL	N
R2	Excellent	Low	N
R3	Excellent	Moderate	N
R4	Excellent	High	N
R5	Excellent	Very High	A
R6	Very Good	NIL	N
R7	Very Good	Low	N
R8	Very Good	Moderate	N
R9	Very Good	High	A
R10	Very Good	Very High	A
R11	Good	NIL	N
R12	Good	Low	N
R13	Good	Moderate	N
R14	Good	High	A
R15	Good	Very High	A
R16	Fair	NIL	N
R17	Fair	Low	N
R18	Fair	Moderate	A
R19	Fair	High	A
R20	Fair	Very High	A

R21	Poor	NIL	N
R22	Poor	Low	A
R23	Poor	Moderate	A
R24	Poor	High	A
R25	Poor	Very High	A

Here, in the output (O/P), N denotes normal nodes and A denotes attack nodes. For every time, the standard base of this FIS framework is to be balanced for each time by altering the information and yield parameters of MFs. In this way, it is basic to decide an optimal mix of these parameters. In this methodology, the accompanying parameters of the FIS framework are to be optimized:

Triangular MFs of the info factors are to be optimized. For instance, if a triangular shape is considered with three peaks esteems, for example, a, b and c as appeared in figure 4, where b and c are fixed while esteem is shifted. In this proposed FIS framework, the info factors TW and ER just have triangular shapes those parameters are to be optimized. As shown in Figure 5, for the input variable TW, three parameters such as x_1, $x_2$and x_3 are to be optimized. Similarly, the input variable RE, three parameters such as y_1, y_2 and $y_3$are to be optimized as shown in figure 6.

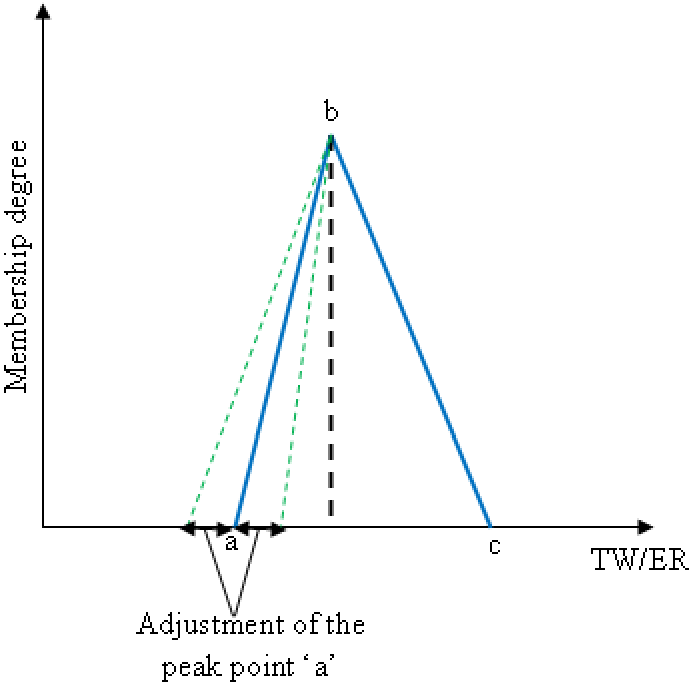

Figure 4: Position of peak points of triangular MF

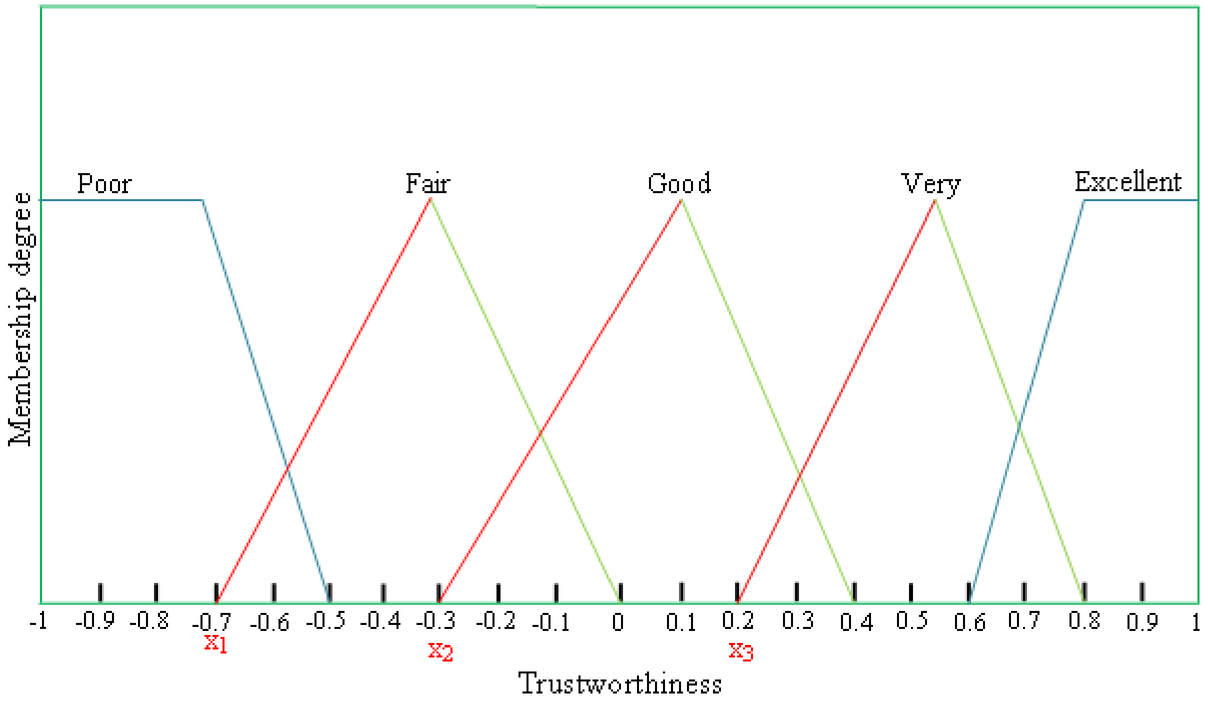

Figure 5: Position of optimized parameters of input variable TW

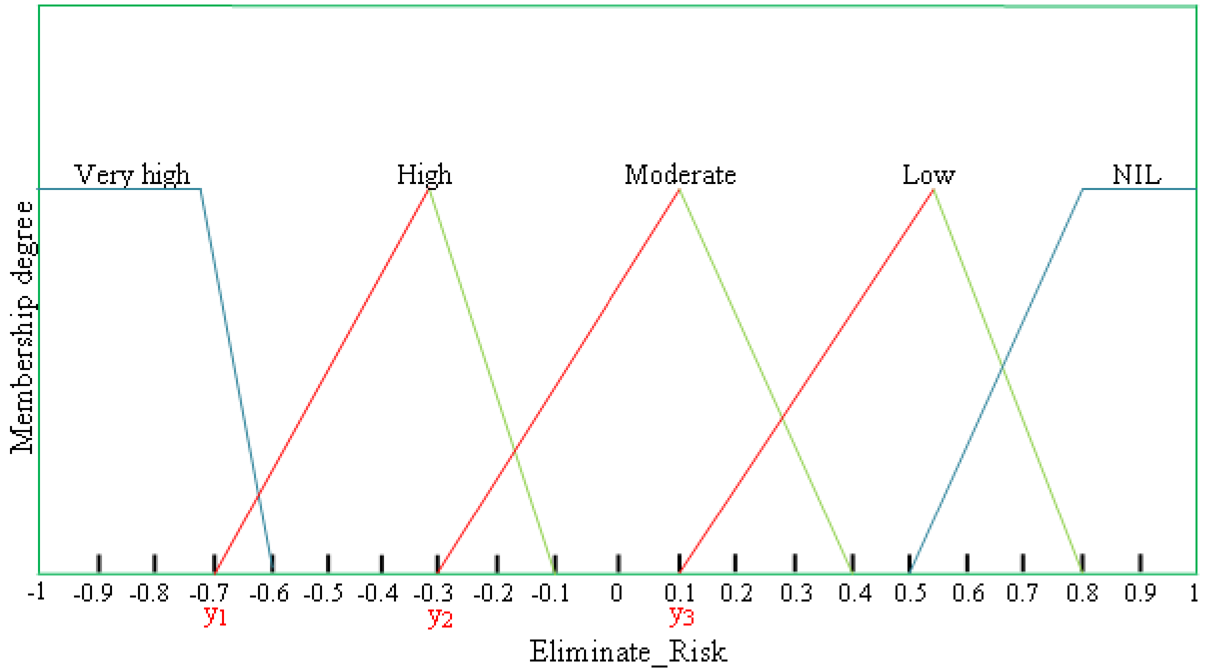

Figure 6: Position of optimized parameters of input variable ER

4. Selecting optimal membership functions using CSO:

For finding the optimal membership function, a meta-heuristic evolutionary optimization algorithm known as CSO is used. This algorithm follows the regular conduct of cats. Cats have good hunting ability and they are highly interested in moving objects. Although cats spend most of their time at rest, they are always alert and move very slowly. When they sense the nearness of prey, they spend a great deal of energy and chase it very quickly. These two qualities, such as (1) resting with slow motion and (2) pursuing with high speed, are denoted by the Seeking and Tracing modes individually, which can be numerically modeled as follows:

Seeking mode involves some new terms such as Seeking Range of selected Dimension (SRD)Seeking Memory Pool (SMP), Counts of Dimension to Change (CDC) and Mixture Ratio (MR).

SMP is the quantity of cat's copy produced in seekingmode.

SRD is the extreme distinction among old and new qualities in the measurement picked for mutation.

CDC is the quantity of measurementsthat are about to be transformed.

Mixture Ratio is a fraction of populace apportioned a little worth. This is to make sure the cats spend most of their energy resting and watching or in seeking mode.

Seeking mode:

i) Arbitrarily choose the MR fraction of cats from the populace as seeking cats and rest of the cats are considered as following cats.
ii) Produce j'th seeking cat's copy.
iii) The situation of each duplicate is refreshed dependent on CDC by including or subtracting SRD fractionof the current position.
iv) Calculate all copies' value of error fitness.
v) Select the best candidate from every one of the duplicatesand place it at the situation of j th seeking cat.
vi) Go to 2nd step till all seeking cats are involved.

$$Q_j = \frac{|FV_j - FV_c|}{FV_{\max} - FV_{\min}}, \ where \ 0 < j < k \tag{4}$$

When the goal of the fitness function is to find the minimum solutions, $FV_c = FV_{max}$, otherwise $FV_c=FV_{min}$.

Tracing mode:

Tracing mode is the sub-model for demonstrating the instance of the cat in following a few targets. When a cat goes into tracing mode, it moves as indicated by its very own speeds for each measurement. The activity of tracing mode can be depicted in 3 phases as pursues:

i) Update the velocities for all the dimensions ($A_{k,h}$ d) using equation (5)
ii) Check whether the velocities are inside the scope of the greatest speed. In the event that the new velocity is in the higher range, set it equivalent as far as a limit.
iii) The situation of cat_k is updated using formula (6)

$$A_{k,h} = A_{k,h} + e_1 \times f_1 \times (z_{best,h} - z_{k,h}), where \ \ h = 1,2,..., M \tag{5}$$

$Z_{best,\ h}$ is the situation of the cat, who has the best wellness value and $z_{k,h}$ is the situation of cat_k. e_1 is a random value within the scope of [0,1] and f_1 is steady.

$$z_{k,h} = z_{k,h} + A_{k,h} \tag{6}$$

The CSO is utilized in the presented system for choosing effective membership functions. The CSO algorithm works based on the natural behavior of the cat. stages of this algorithm are described as bellows:

Initialization:

i) Initialize the initial population of cats. Here, the solution set is referred to as a cat.

ii) Position the cats arbitrarily in the *g* dimensional arrangement space and arbitrarily choose esteem that is within the limit of most extreme velocity, to the velocities of every cat.

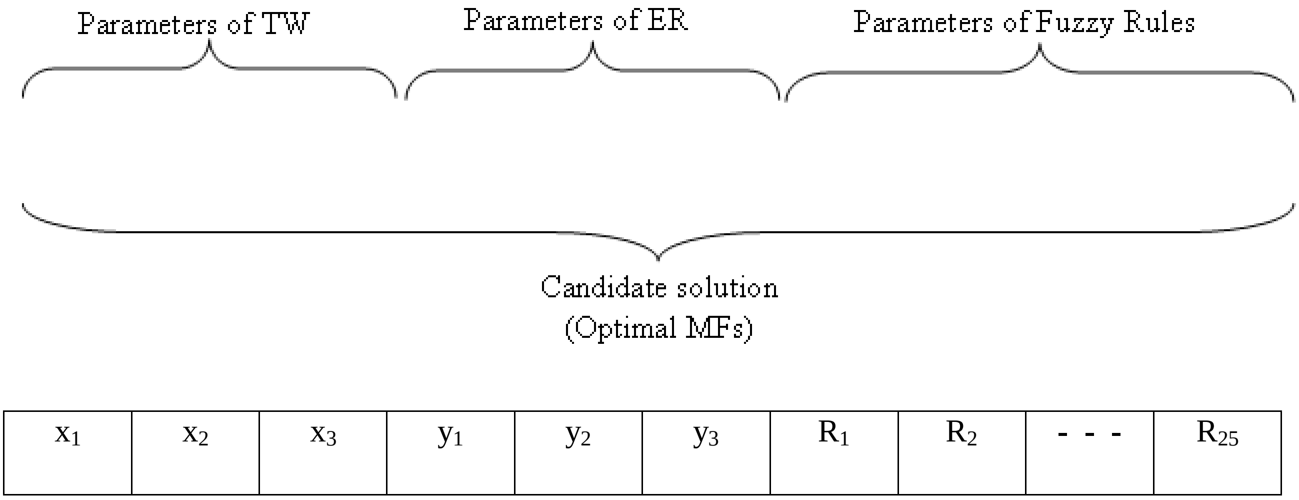

Figure 7: Structure of the solution

Let the candidate solutions or cats are introduced in *g* dimensional space as pursues,

$$Z = \{MF_1, MF_2, ..., MF_g\} \tag{7}$$

Here, the position of the cat or optimal membership function in g^{th} dimension is represented as MF_g.

Fitness evaluation:

iii) The fitness of the cat or candidate solution is calculated after the initialization of the cat or candidate solution. The framework with higher accuracy is chosen as an optimal fuzzy framework. It can be determined using equation (8).

$$Fit_k = Min\{ACC_k\} \tag{8}$$

Here, the accuracy of the k^{th} solution is denoted by Fit_k. And the accuracy can be evaluated using equation (9).

$$ACC_k = \frac{US + UT}{US + UT + VS + VT} \tag{9}$$

Here, US represent true positives, UT represents true negatives, VS represents false positives and VT represents false negatives.

Updating the solution:

iv) Update the best cat or best solution into the memory. The position of the best solution alone is required to be stored in the memory as it can lead to the best solution to that point.

v) The solutions or cats are moved based on their flags. Check whether the cat is in tracing mode orseeking mode. Using equation (4), the cat is applied to the seeking process if it is found that the cat is in tracing mode. If the cat is found to be in tracing mode, then the cat is applied to the seeking mode process using equation (6).

vi) In the next step, the numbers of solutions are re-picked. Based on MR, these re-picked solutions are set into tracing mode and the remaining solutions are set into seeking mode.

Termination:

vii) The condition for termination or the end criterion is checked and if the condition is not satisfied, then the steps from the fitness evaluation are repeated till the condition is satisfied. If the condition is satisfied, the program is terminated and the best solution is provided as the output.

5. Result and discussion:

The proposed approach's simulated outcomes are provided in this segment. The proposed approach's performance is compared with the performance of the existing fuzzy system approach in terms of delay,energy consumption, throughput, delivery ratio and network lifetime

.

5.1.Experimental setup:

The CatSwarm Optimization based FSA approach for group key management is actualized in the platform of MATLAB R2015a with the framework having an i3 processor and 8GB RAM. Table 4displays the simulation-parameters and assumptions.

Table 4: Simulation parameters

Number of nodes	100
Area	1000 x 1000
MAC Simulation Time	500 sec
MAC	802.11
Number of attackers	Between 0 to 10
Traffic source	CBR
Antenna	Omni antenna
Pause time	100 m/s
Initial energy	15 J
Power Transmission	0.770
Receiving power	0.425
Propagation	Two ray ground reflection model

5.2.Performance analysis:

Figure 8 shows the execution of the proposed approach and compared the existing approach in terms of delay. The delay of a system has to be low for it to function effectively. When the number of nodes is 20, the delay on the proposed AFS approach is 160ms and the delay of the existing FS approach is 175ms. The delay of the proposed system is 262ms and the delay of existing FS is 750ms when the number of nodes is 40. The proposed AFS approach has lower delay than existing FS system. The order of delay is same for all the number of nodes. From the graph it can be clearly known the proposed AFS approach has performed greater than the existing FS approach.

Figure 9 shows the execution of the proposed AFS approach and the existing FS approach in terms of delivery ratio. The delivery ratio has to be high for a system to be effective. The delivery ratio of the proposed AFS approach is 41 and the delivery ratio of the existing FS approach is 9 when the number of nodes is 40. When the number of nodes is 80, the proposed AFS approach by delivery ratio is 78 and the delivery ratio of the existing FS approach is 16. The delivery ratio of the proposed approach is higher than the new approach. This condition is same for all the number of hubs. From the graph, it can be clearly seen that the proposed AFS approach has performed greater than the existing FS approach in terms of delivery ratio.

The energy consumption based execution of the proposed AFS approach and the existing FS approach is shown in Figure 10. The energy consumption has to be low for the system to function efficiently. When the number of nodes is 60, the energy devoured by the proposed AFS approach is 10J whereas the energy consumed by the existing FS approach is 61.7J. When the number of nodes is 100, the energy consumed by the proposed AFS approach is 31J whereas the energy consumed by the existing FS approach is 80J. The energy devoured by the proposed AFS approach is lower than the energy consumed by the existing FS approach. The condition is same for all the number of nodes. It can be clearly understood from the graph that the proposed AFS approach has performed greaterthan the compared existing FS approach in terms of energy utilization.

The network lifetime based performance evaluation of the proposed AFS approach and the existing FS approach is shown in Figure 11. For a system to be effective, the network lifetime of that system must be big. When the quantity of hubs is 20, the network lifetime of the proposed AFS approach is 266 and the network lifetime of the existing FS approach is 21. When the number of nodes is 60, the network lifetime of the proposed approach is 78 and the network lifetime of the existing FS approach is 10. The network- lifetime of the proposed AFS approach is higher than the compared FS approach. This condition is the same for all the number of nodes. It can be clearly seen from the graph that the proposed AFS approach has performed greater than the existing FS approach in terms of network lifetime.

The proposed AFS approach's and the existing FS approach's throughput based performance is shown in Figure 12. The system with higher throughput is considered as an efficient system. When the number of node is 80, the throughput of the proposed AFS approach is 121kb/s and the throughput of the existing FS approach is 81kb/s. Likewise, when the number of node is 100, the throughput of the proposed AFS approach is 102kb/s and the throughput of the existing FS approach is 86kb/s. Here, the throughput of the proposed AFS approach is bigger than the throughput of the compared FS approach. This condition is same for all the number of nodes. From the graph, it can be known that the proposed AFS approach has performed greater than the existing FS approach in terms of throughput.

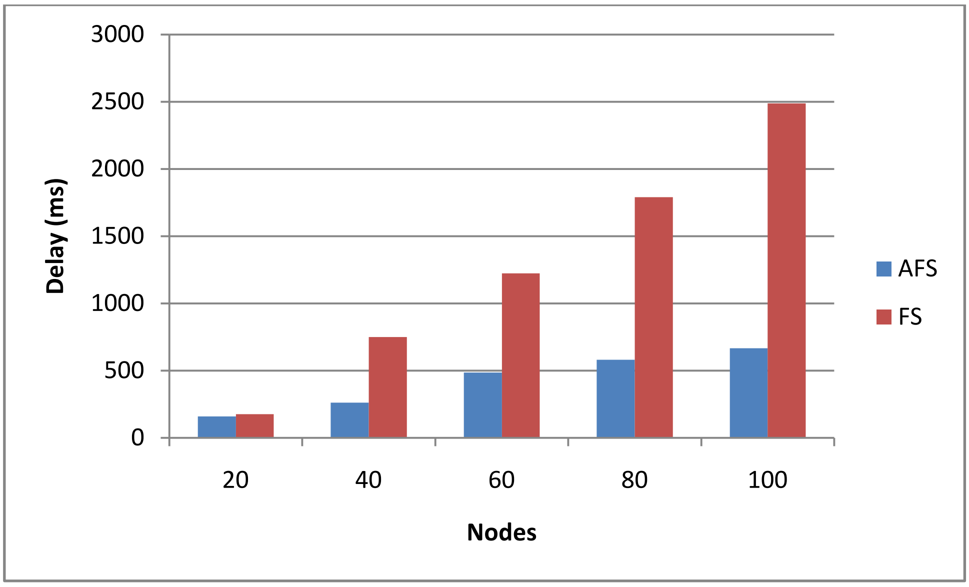

Figure 8: Delay based performance analysis of AFS and FS approaches

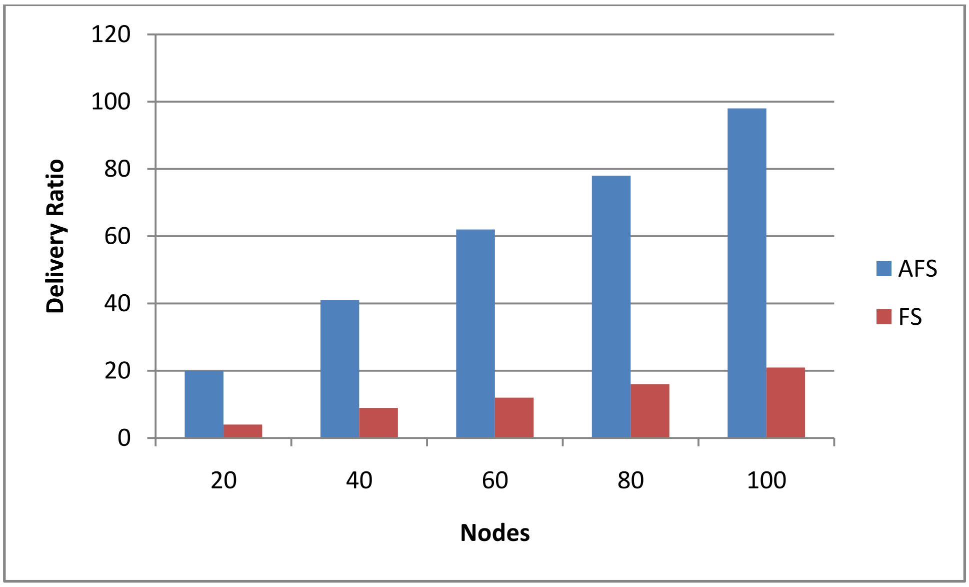

Figure 9: Delivery ratio-based performance analysis of AFS and FS approaches

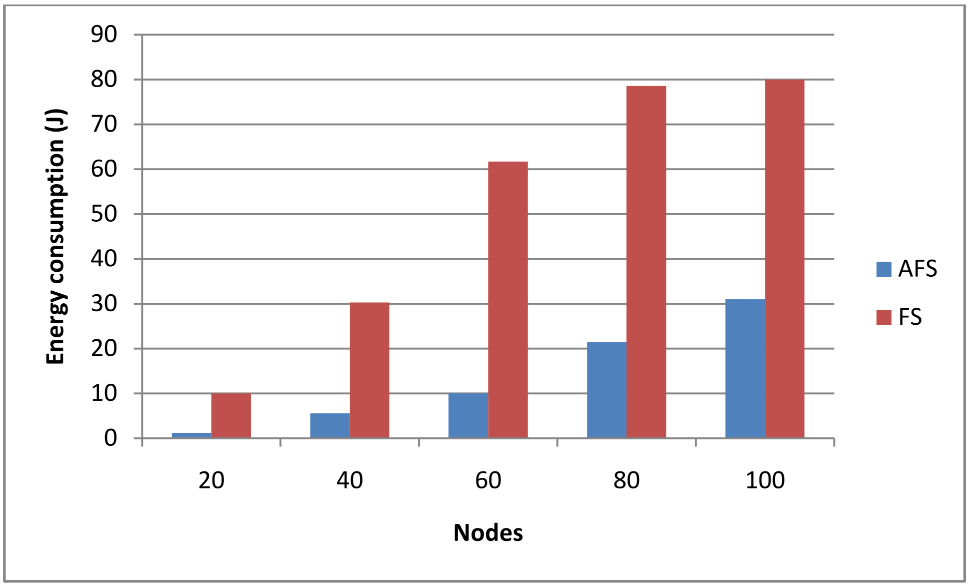

Figure 10: Energy consumption based performance analysis of AFS and FS approaches

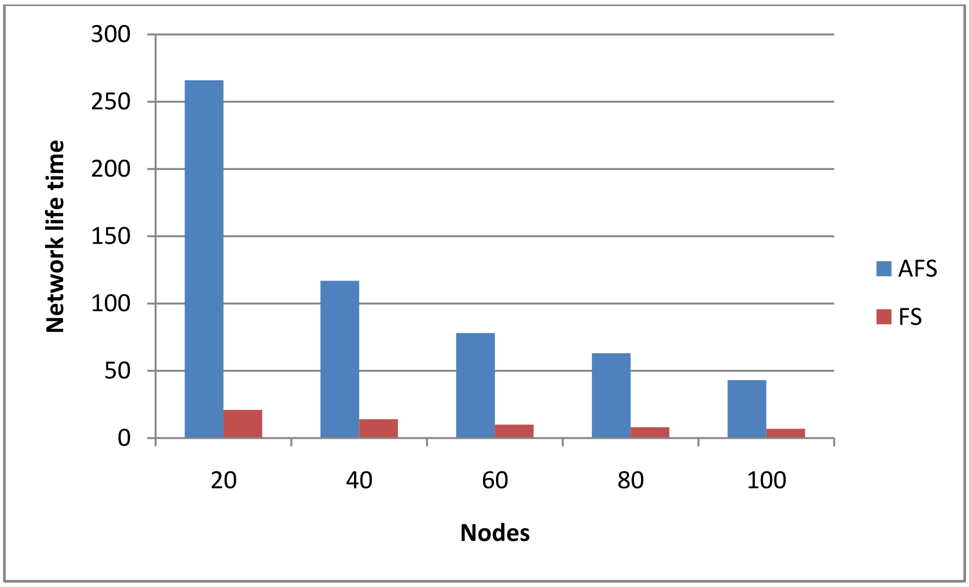

Figure 11: Network life time-based performance analysis of AFS and FS approaches

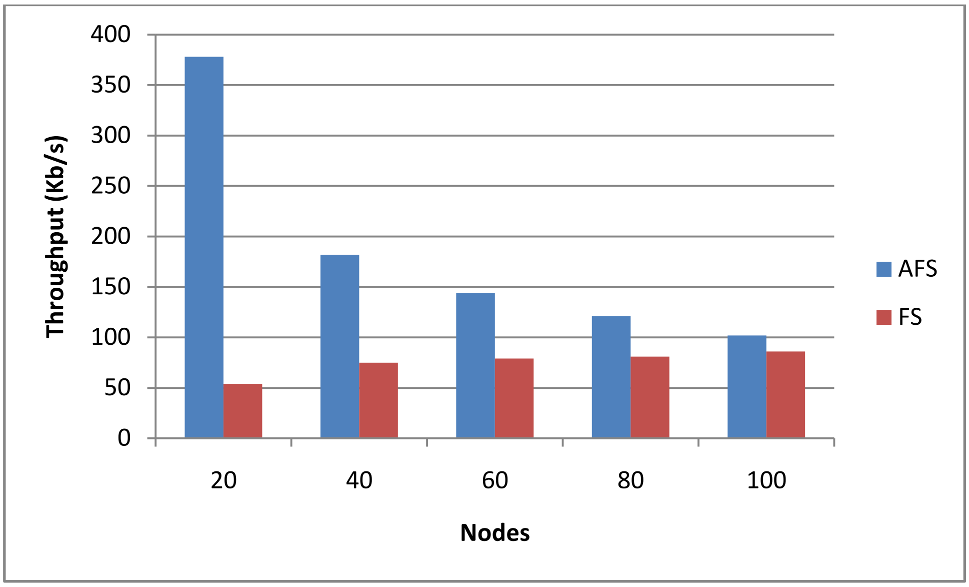

Figure 12: Throughput based performance analysis of AFS and FS approaches

6. Conclusion:

An Adaptive Fuzzy System based Insider Attacks detection with Group Key management is presented for wireless ad hoc network.The CSO algorithm has been utilizedto select optimal membership functions. At first, the clusters are formed and the cluster heads are chosen dependent on the trust values and node mobility. The chosen cluster head provides group key to the group members. An adaptive fuzzy system is utilized to find and destroy the misbehaving nodes. The CSO is utilized in finding the optimal membership functions. The results have been simulated for the proposed approach and the result is compared with traditional fuzzy system approach. The execution of the proposed approach is analyzed in terms of delay,energy consumption, delivery ratio, network lifetime and throughput. On comparing performance of the proposed and existing approaches, it is clear that the proposed AFS-CSO approach has performed much better than the existing FS approach.

Reference:

[1]. Vasudeva, A., &Sood, M. (2018). Survey on sybil attack defense mechanisms in wireless ad hoc networks. Journal of Network and Computer Applications, 120, 78–118.

[2]. Madhja, A., Nikoletseas, S., &Voudouris, A. A. (2019). Adaptive wireless power transfer in mobile ad hoc networks. Computer Networks, 152, 87–97.

[3]. Rahdar, A., &Khalily-Dermany, M. (2017). A schedule based MAC in wireless Ad-hoc Network by utilizing Fuzzy TOPSIS. Procedia Computer Science, 116, 301–308.

[4]. Yusop, Z. M., &Abawajy, J. (2014). Analysis of Insiders Attack Mitigation Strategies. Procedia - Social and Behavioral Sciences, 129, 581–591.

[5]. Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., & Goldsmith, M. (2015). Identifying attack patterns for insider threat detection. Computer Fraud & Security, 2015(7), 9–17.

[6]. ZhifengLuo,& Chen Liang. (2016). An insider attack on shilling attack detection for recommendation systems. 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS).

[7]. Kim, J.-S. (2011). Development of Integrated Insider Attack Detection System Using Intelligent Packet Filtering. 2011 First

ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering.

[8]. Tong, S., Li, Y., & Sui, S. (2016). Adaptive Fuzzy Tracking Control Design for SISO Uncertain Nonstrict Feedback Nonlinear Systems. IEEE Transactions on Fuzzy Systems, 24(6), 1441–1454.

[9]. Wu, C., Liu, J., Jing, X., Li, H., & Wu, L. (2017). Adaptive Fuzzy Control for Nonlinear Networked Control Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 47(8), 2420–2430.

[10]. KhaledSaifullah, C. M., &Rafiqul Islam, M. (2016). Chemical reaction optimization for solving shortest common supersequence problem. Computational Biology and Chemistry, 64, 82–93.

[11]. Wang, N.-C., & Huang, Y.-C. (2015). An SDMA-based MAC protocol for wireless ad hoc networks with smart antennas. Computers & Electrical Engineering, 41, 383–394.

[12]. Li, K.-H., &Leu, J.-S. (2015). Weakly connected dominating set-assisted ant-based routing protocol for wireless ad-hoc networks. Computers & Electrical Engineering, 48, 62–76.

[13]. Yao, W., Han, S., & Li, X. (2015). LKH++ Based Group Key Management Scheme for Wireless Sensor Network. Wireless Personal Communications, 83(4), 3057–3073.

[14]. Meng, W., Li, W., Xiang, Y., &Choo, K.-K. R. (2017). A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks. Journal of Network and Computer Applications, 78, 162–169.

[15]. Meng, W., Li, W., Wang, Y., & Au, M. H. (2018). Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. Future Generation Computer Systems.

[16]. Akram, M., & Cho, T. H. (2016). Energy efficient fuzzy adaptive selection of verification nodes in wireless sensor networks. Ad Hoc Networks, 47, 16–25.

[17]. Chen, S.-L. (2015). A Power-Efficient Adaptive Fuzzy Resolution Control System for Wireless Body Sensor Networks. IEEE Access, 3, 743–751.

[18].