Fuzzy Logic Based Technique using Trust Authentication for a Secure Data Exchange in Wireless Sensor Networks

Blessey.P.M[#1], R.Geetha[#2]

[#1]*PG Scholar, Computer Science Department, S. A. Engineering College, Anna University*
Chennai, Tamilnadu, India

[#2]*Associate Professor, Computer Science Department, S. A. Engineering College, Anna University*
Chennai, Tamilnadu, India

Abstract**—**Secure links are established between the nodes to provide guaranteed high security, integrity and better performance in wireless sensor network. In order to achieve secure link between the nodes, the concept of trust and certification authority is integrated to combat against the misbehaving entities to deal with the security challenges. The fuzzy based technique is employed by the cluster head to differentiate the nodes as trusted or malicious by issuing the services only to the trusted node and eliminates the misbehaving nodes. The proposed scheme is more reliable and provides improved security in military network. Existing random seed distribution with transitory master key scheme – a hybrid approach of random key distribution and transitory master key may provide the resilience and the connectivity but still the security is degraded, if the secret key is compromised. Even though a number of key management schemes have been used, none of them are satisfactory. Compared to the existing scheme, the PROPOSED scheme provides better security features but also ensures enemy intruders to stay away from the network. Hence, it offers good communication with sufficient connectivity among the nodes; hence it could be used in military and remote area communication.

Keywords**—** Fuzzy logic, Securing Military Network, Trust, Key Management, Misbehaving node detection

I. Introduction

Wireless Sensor Network such as military, industrial network is susceptible to certain attacks such as data modification, eavesdropping [1] and [7]. Current trend is the communication between portable sensor devices. Trust expresses the behaviour of the entities as degree of belief. Misbehaviours and non-cooperative actions among the nodes in the network will ruin the reputation or trust value for trust bond establishment between the nodes. Trust and Fuzzy Logic techniques employed, helps in managerial to improve security, robustness and detection of adversary nodes [4]. The challenges that appear in wireless sensor network is that network is vulnerable to all kinds of attacks initiated due to compromised node and battery power in mobile devices causes trade-offs between security. Battery Depletion of the nodes trade-offs between resource utilization and security of the device.

Key management was one of the mostly used techniques for secure communication but each emerging scheme in key management is limited with the compromised node. The main disadvantage is that the compromising nodes would generally lead to the dreadful conditions of the network by security degradation [2]. Hence, either the resilience or the connectivity is limited in the network. Moreover, Fuzzy logic based technique using trust authentication helps to find the trusted and illegitimate nodes in the network [8].

II. Related Work

In this section, we discuss the limitation of the latest key management approaches and represent the techniques related to the proposed scheme

A. Random seed distribution with transitory master key scheme:

Random seed distribution with transitory master key provides large number of key from a small pool. RSDTMK scheme can be used to generate all types of keys such as individual key, cluster key, global key and pair wise key. Prior to network deployment, each node receives the parameters and the configuration is completed. Each node contains the secret material for the key generation. The two phases of this approach is the initialization and working phase. At first, during the initialization phase, keys are generated by transforming seed with the help of confidential material. In the working phase, keys produced from the previous phase are used and this phase is used for scalability purpose by addition of nodes in the network. Latest RSDTMK key management scheme provides better security compared to the other scheme, yet it compromises the secret material and the nodes in the initialization phase still cause security problems

B. Polynomial pool based key pre-distribution scheme:

Polynomial pool based key pre-distribution generates bivariate polynomial and distributes a subset of polynomial to each ring. Three phases of this technique are the setup phase, direct key establishment phase and path key establishment phase. This approach is secure only up to t compromised nodes, but it cannot tolerate more than t compromised nodes in the system. Random subset assignment schemes and the Grid based key pre distribution schemes are the classification of the Polynomial pool based key pre-distribution scheme which provides secure communication when there is no compromised node or when the compromised node doesn't exceed the threshold value. Hence, the secure communication is being doubtful due to the node compromisation problem.

C. Transitory master key scheme:

In this approach, the master key is pre-configured in the nodes deployed in the network. To achieve protected service, nodes share the master key with the neighbour nodes. The master key is erased from its memory after a time period. The adversary can easily retrieve the information, if the master key is stored in flash memory or even in volatile RAM. If the master key is compromised before it has been wiped away, then the attacker will obtain every generated pairwise key. Hence, the single point of failure occurs in the sensor network. This leads to a lot of misbehaving nodes in the network.

D. Trust Management Framework

In the trust management framework consists of three components. The Trust agent obtains trust level from its behaviour that is directly experienced by a node. Trust Agent exists in every node and achieves the task of quantification, computation and trust derivation. Recommendation agent shares the trust information about nodes with its neighbour nodes in the set-up. The agent sends recommending information to other requesting nodes. The component Combiner, calculates the final trust value of a node based upon the information obtained from both the agents. The Combiner calculates trust values by combining the results of Trust agents and Recommendation agents [3].

E. Fuzzy Logic Based Trust Levels

Fuzzy logic Technique provides accurate outcome rather than fixed and approximate. Fuzzy logic variables of trust values are in the range of degree from 0 to 1. If the trust value obtained for a node is greater than or equal to the threshold value, then that node is called as a trustworthy, but if the trust value is less than the threshold trust value then the node is called as untrustworthy. Based on the node's trustworthiness, the node can be incorporated in the network operations such as transmitting/ receiving data and routing packets. Trust levels in fuzzy logic are represented in ranges from very untrustworthy to very trustworthy levels with the set of values. The trust value of node is of two types such as trustworthy and untrustworthy.

III. Attacks

This section represents the attacks in the network and functioning of the attack [10].

A. Data Modification Attack

Modification attack is an attack which not only achieves access to the data but also alters for the sake of benefit. It redirects network traffic and performs DOS attacks by altering the fields of the message or by forwards routing message with fake values.

B. Masquerade Attack

Since the authentication of data packets in ad-hoc network security is brittle, since a misbehaving node can initiate several attacks in a network by faking to be legal node. Spoofing is an example that takes place when a malicious node fakes its identity in the network i.e. by altering its IP address or MAC with the identity of other trusted node in outgoing packets.

C. Fabricated Attacks

Fabrication attack achieves the authorized access injects counterfeit objects into the set-up. The Fabrication attack may lead to false routing messages to perform attacks.

D. Gray Hole Attack

Gray hole attack promotes its route as a legal path by intercepting the packets. The packets are dropped, when it pass through the malicious node. It's hard to find these attacks since it exhibits different behaviour to different nodes. Packet dropping and modification are the main parameters of this attack.

E. Worm Hole Attack

A wormhole attack makes sure that the tunnelling process is followed. Cluster of nodes work together to encapsulate and exchange data between them. Normal flow of packets is short circuited as no packets are permitted in the path. This kind of attack consumes energy of the node at great extent. Packet delay and Energy are the parameters involved in this attack.

F. Black Hole Attack

The malicious node announces the path as a valid path to the destination node and interrupts every packet from forwarding and can produce phony information is known as the blackhole attack. Blackhole attack modifies the packet content and the packet delay is occurs without forwarding.

G. Jellyfish Attack

Jellyfish attack joins the forwarding group of nodes and delays the packets for a specific time unreasonably and then the packet is forwarded. This kind of attack can drastically reduce the network performance and increase the traffic flow of packets.

H. Denial of Service Attacks

Denial of service attacks disrupts the routing function but also the entire process in the network. Specific occurrence of denial of service attack comprises of the routing table overflow and the sleep deprivation torture. Routing table overflow attack is nothing but the flooding the entire network with malicious node, consuming the resources. Packet modification and re-routing are the parameters of denial of service attack.

I. Rushing Attack

When the source node sends the “route request” to the attacker node, it floods the packet rapidly all over the network prior to other nodes which as well receives the same “route request” Even though the nodes receives the genuine route request packet, it believes that the packets are the replica of those that are send or forwarded by the attacker node and thus reject those packets. Route request packet duplicates and modification are the parameters.

J. Resource consumption Attack

An attacker node intentionally attempts to consume the resources such as battery power of other nodes in the network. Attacks might be in any form of unnecessary route request control messages, forwarding of stale information to nodes or very frequent generation of beacon packets. Packet modification and energy are the parameters that can very much identify this attack.

IV. Secure Communication Using Trust And Fuzzy Logic

This section describes the components of the proposed framework and its role of responsibility.

A. Energy Value

In Ad hoc network, initially nodes have maximum energy i.e. with full battery. Later, energy is consumed as the communication begins such as when the data packets forwarded to the neighbouring nodes and received by it. In the trusted nodes, the energy consumption is normal as the packets are received as well as forwarded by them that are requested whereas the malicious node utilizes more energy since those nodes receive the data packets, modifies them and forwards packets which occur more often in the network [2], [5], [9]. To calculate the residual energy, node configuration is necessary that contains initial energy, ideal power consumption, power consumption during transmission and receiving.

B. Direct and Indirect Trust Value

Trust value is a combination of direct trust value and indirect trust value [8]. Direct trust value is calculated by monitoring the performance of neighbouring node whether it is behaving in a normal or abnormal way. Every node directly observes the neighbour nodes by listening to the communication, detects packet dropping, delay in packet transmission and packet forwarding. Direct trust value is stored in the trust table, which comprised of node position, direct trust value and total trust value of the corresponding node. Indirect trust value is obtained by the recommended trust value from the neighbour nodes. The major task of recommended trust is to gather trust information about the corresponding node from the neighbouring nodes. The source node broadcasts the recommendation request to all of its neighbouring nodes. The reply is received from the requested node, if the source node has direct trust value on the target node. Thus, the fuzzy logic is applied to the direct trust value of all the neighbours’ nodes that are replied to request [12], [15].

C. Final Trust Value

The final trust value is calculated using the energy and trust value of the target node. With the values obtained, total trust value of each node is calculated and timeout value is allotted. Therefore a node trust table is generated with the records containing node it, trust type, trust value and the timeout of the trust. The cluster head requests to compute trust for the node, when the trust value of the node gets expired. Trust table updation occurs each time, when the trust is computed.

D. Fuzzy Logic

Trust level symbolizes node’s behaviour as the positive experience increases the trust level of the node and negative experiences decreases the trust level [2]. Fuzzy logic offers the ability to handle doubt and vagueness effectively. The Fuzzy logic based technique computes the trust value of node. Trust values are calculated based on the final trust value Trust values are calculated based on Trust values are calculated based on the final trust value as a product of energy value and the trust value. These values are inputted as fuzzy input variables and the trusted and malicious node is detected and marked using the Fuzzy logic based algorithm [11],[13],[15]. Fuzzy logic based algorithm works during the nodes request for data exchange.

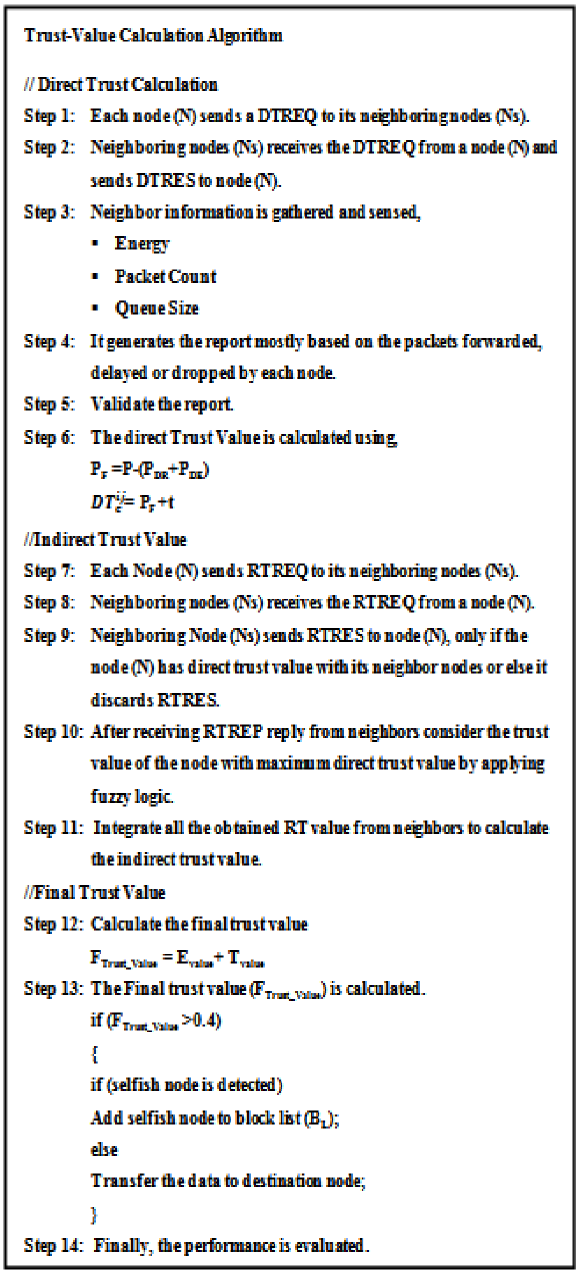
E. Secure Transmission

Integration of trust level and fuzzy based technique provides secure transmission. If the node requesting the data exchange is TRUSTED then the data communication is provided to the requested node. A VERY HIGH, HIGH, and MEDIUM fuzzy value of a node comes under the TRUSTED kind of node. Fuzzy Logic defines whether the node is trusted or not. Hence, trust and fuzzy values helps TRUSTED node to exchange the packets. Check the trust values of each node and update it periodically.

F. Malicious Detection

LOW, VERY LOW fuzzy values of a node are treated as MALICIOUS. The fuzzy logic based Technique detects the malicious nodes in the network. If the node requesting the communication is found to be MALICIOUS then the node that has been requested for communication denies the service. Thus, prevents the selfish nodes from taking part in the activities of the network. The cluster head vibrates an alarm to indicate the trusted nodes in its range about the node's selfish behaviour. Moreover, the malicious node is isolated and a secure network is provided [10]. Thus, less trusted malicious nodes cannot cause threats in the proposed scheme.

ALGORITHM I
TRUST-VALUE CALCULATION AND DETECTION



```
Trust-Value Calculation Algorithm

// Direct Trust Calculation
Step 1:   Each node (N) sends a DTREQ to its neighboring nodes (Ns).
Step 2:   Neighboring nodes (Ns) receives the DTREQ from a node (N) and
          sends DTRES to node (N).
Step 3:   Neighbor information is gathered and sensed,
            ▪ Energy
            ▪ Packet Count
            ▪ Queue Size
Step 4:   It generates the report mostly based on the packets forwarded,
          delayed or dropped by each node.
Step 5:   Validate the report.
Step 6:   The direct Trust Value is calculated using,
          $P_F = P-(P_{DR}+P_{DE})$
          $DT_t^{ij} = P_F + t$
//Indirect Trust Value
Step 7:   Each Node (N) sends RTREQ to its neighboring nodes (Ns).
Step 8:   Neighboring nodes (Ns) receives the RTREQ from a node (N).
Step 9:   Neighboring Node (Ns) sends RTRES to node (N), only if the
          node (N) has direct trust value with its neighbor nodes or else it
          discards RTRES.
Step 10:  After receiving RTREP reply from neighbors consider the trust
          value of the node with maximum direct trust value by applying
          fuzzy logic.
Step 11:  Integrate all the obtained RT value from neighbors to calculate
          the indirect trust value.
//Final Trust Value
Step 12:  Calculate the final trust value
          $F_{Trust\_Value} = E_{value} + T_{value}$
Step 13:  The Final trust value ($F_{Trust\_Value}$) is calculated.
          if ($F_{Trust\_Value}$ >0.4)
          {
          if (selfish node is detected)
          Add selfish node to block list ($B_L$);
          else
          Transfer the data to destination node;
          }
Step 14:  Finally, the performance is evaluated.
```

Hence, the nodes are differentiated as trusted or malicious based on the trust and energy value. Furthermore, routing is performed based on the trust; enhancements are made in the routing protocols to support trust such as trusted AODV and trusted GSPR, which have been widely addressed [6].

1) Trusted AODV: It is an extended version of AODV routing protocol to achieve routing by including the trust metrics. Therefore, the trust is recommended and the routing decision policy of AODV routing protocol is modified. A set of policies of a node results in updating its opinions towards other nodes in the network, as it is essential to design a trust information exchange, when applying the trust models into network.

2) Trusted GPSR: Greedy Perimeter Stateless Routing is enhanced as it uses trust levels of node. Each time a node sends packet it remains still until it gets information whether its neighbouring node is forwarding the packets or not. Thus, the trust value for its neighbours is maintained based on the accurate forwarding information and these data are used for the routing decision.

3) *Trust- Aware DSR:* Dynamic Source Routing protocol is secure routing by incorporating certain mechanism for security purposes. These mechanisms help for detecting selfish nodes which do not forward packets. For the detection function, each node in the network set-up buffers every transmitted packet for a short time period. Thus, each node gets in the licentious mode to find out whether the neighbour nodes have forwarded the packet or not. Hence, nodes are rated based on the feedback received, which indeed used to choose routes with the highest forwarding rate

G. Benefits of the proposed system

Fuzzy logic based technique using trust authentication for a secure data exchange is more effective and efficient than the existing key management scheme, since there is no chance of compromising node occurs here. In the proposed scheme, we doesn't need to be troubled about whether the node has been compromised by an adversary as only the trusted nodes are allowed for communication. Key management schemes are the complex techniques used to provide security but still the probability of compromising nodes in the network cannot be eradicated. In this system, nodes cannot be compromised; nodes are declared trusted based on the behaviour. Misbehaving nodes can perform a good behaviour for a limited time but not throughout the service, since the nodes trust value is calculated and updated in the routing table for a minimum time period. However, the malicious nodes are detected and eliminated from the service.

Instead of using traditional security approaches that are complex in nature, to eliminate security vulnerabilities. We introduce a simple technique of updating routing table using trust values of node to have a maximum network performance. Trust management system increases the expressiveness, flexibility and scalability of the network. It provides better network performance using linguistic fuzzy sets as input.

Integrated technique of trust and fuzzy will be very much helpful in detecting misbehaving nodes and for supporting in the process of decision making. Moreover, the trustworthiness of the nodes is estimated from its past and current behaviours. It mainly assists in testing the integrity of a suspected node. In Wireless sensor networks, the number of members is of thousands of nodes. Based on the lifetime of the network, the network should provide services for much longer periods of time. Hence, trust value should be updated periodically or it may affect the trust progression on the network.

Therefore, this work includes the proposed system analysis with the most commonly used routing protocols to identify malicious nodes and prevents the network from certain security attacks.

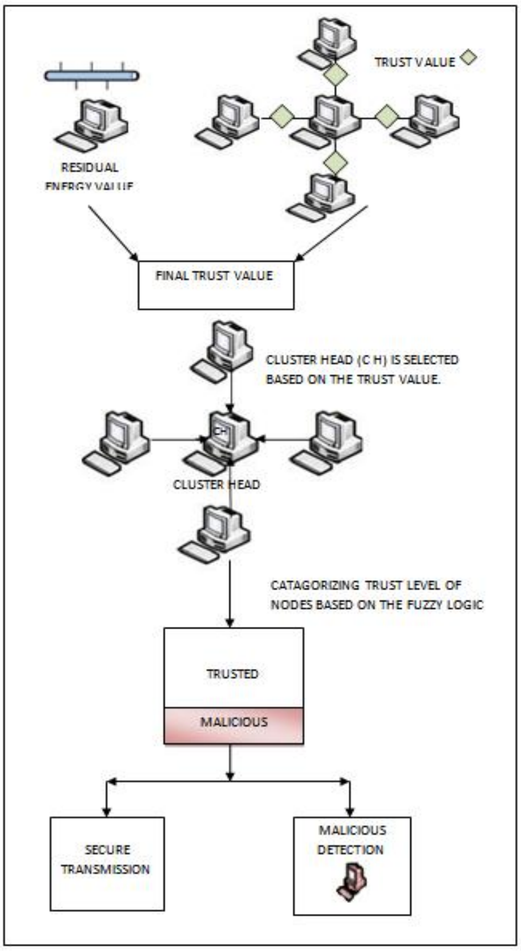


Fig. 1 Structure of Proposed System

V. Comparative Study

The Fuzzy based technique using trust authentication [3], proposed system that provides the secure data exchange effectively with the help of trustworthy nodes in the network.

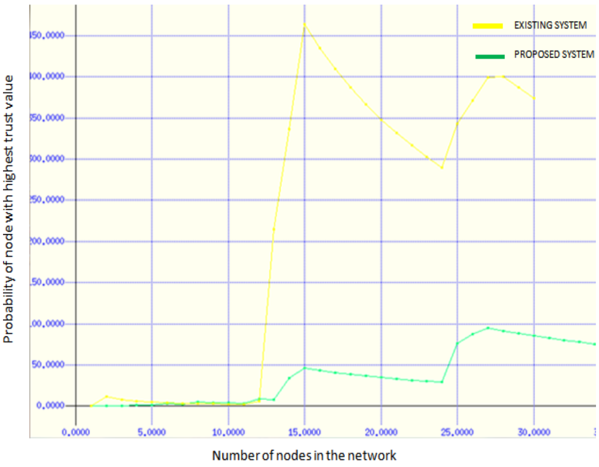


Fig. 2 Comparison study between the existing and proposed schemes to find the nodes with highest trust value

Fig.2 depicts that the comparison between the existing key management and the proposed fuzzy based technique using trust authentication scheme that indicate the proposed system has network of highest number of trust value nodes. The network consists of most probably trustworthy nodes in the network by using three main important components such as trust value, energy value and fuzzy logic.

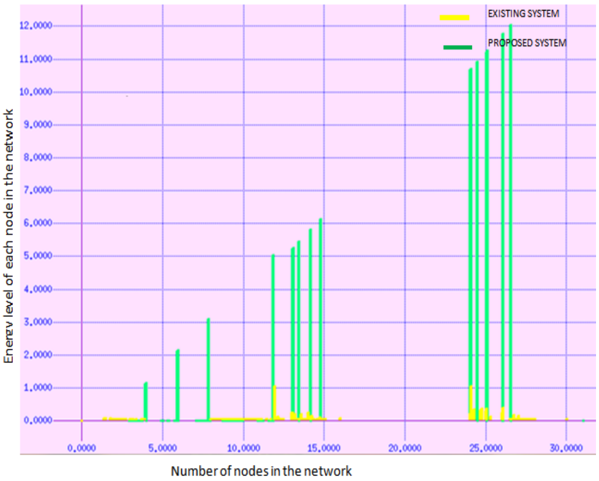


Fig. 3 Probability of residual energy available in each node

The graph describes the available energy retained by nodes in the network. The sensor nodes regularly uses limited energy sources such as batteries. Some of the major reason of energy utilization in typical sensor network is that the communication between the nodes is not continuous due to the connection problem. On the other hand the energy depletion in the WSN is due to the idle mode consumption, such that when the node is not transmitting or receiving any information from other nodes but just listening and waiting for information from other nodes. The energy available in each network helps in selecting the cluster head node. The node with high energy value in combination with high trust value provides data exchange in the network as shown in the fig.3.

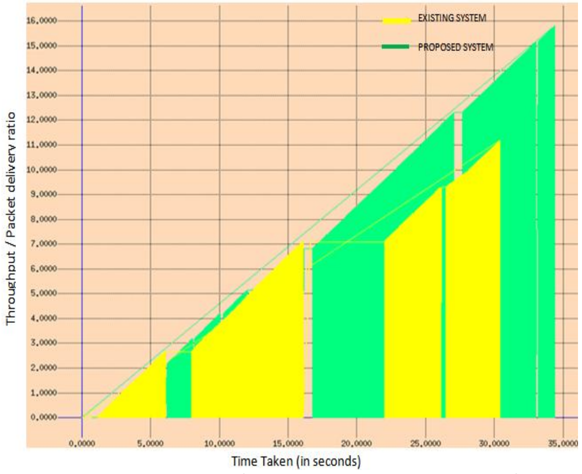


Fig. 4 Simulation results of packet delivery ratio at a specified time period

The Fig.4 denote graphical representation that symbolizes the delivery ratio of packets in both the existing and proposed scheme, where there is drastic increase in the packet delivery ratio in the proposed fuzzy based trust authentication technique in a given time period. When the connection is stable with trusted nodes in the network, then the packet is forwarded or received within the time interval. The rate at which the proposed protocol is effective than the existing scheme is described in fig.5.

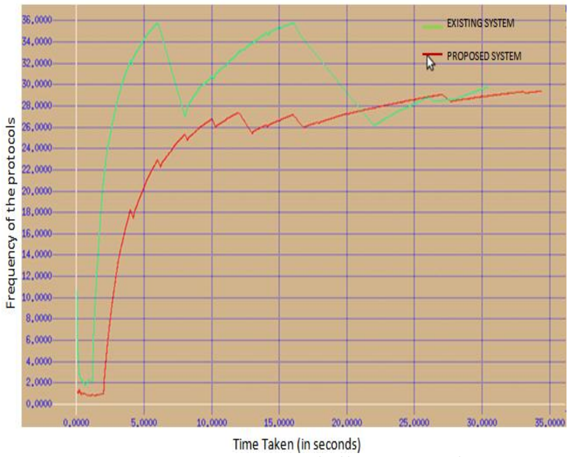


Fig. 5 Graphical representation of effectiveness of the scheme

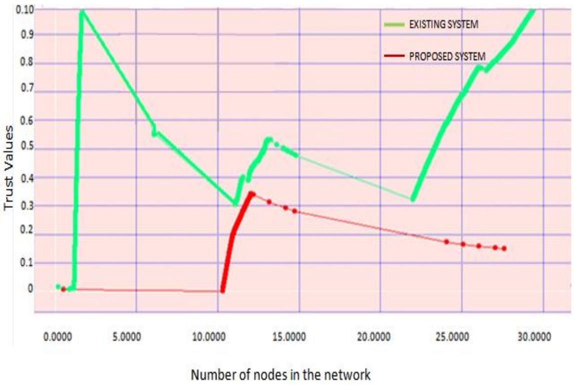


Fig. 6 Simulation results indicating trustworthiness of each node in the network

A comparative study is completed with the existing method to the proposed framework. We have taken existing system that describes key management to compare with the proposed scheme featuring Direct and Indirect Trust for malicious node detection and Fuzzy Logic. The proposed framework identifies every malicious nodes in the network based on the final trust value generated by the sum of trust value and energy value. Nodes are said to be malicious node when the trust value falls below the threshold. Comparative study of various test cases with the existing and proposed techniques has revealed that proposed method is more accurate and reliable and the chances of distinguish malicious node is higher in the proposed scheme.

TABLE II
TRUST VALUES FOR THE TRUSTED AND MALICIOUS NODES IN THE NETWORK

Fuzzy levels	Trust Values	Semantics
1.very high	0.8 to 1	Trustworthy
2.high	0.6 to 0.8	Trustworthy
3.medium	0.4 to 0.6	Trustworthy
4.low	0.2 to 0.4	Untrustworthy
5.very low	0 to 0.2	Untrustworthy

VI. CONCLUSIONS

Wireless Sensor Network comprises of several mobile devices with varying performance capabilities. Each and every model proposed for wireless sensor networks should not involve unrealistic communication and computation requirements. During network deployment, security appears as a vital requirement since there are various attacks that affect the network performance. The proposed technique suggests a strong network by considering the characteristic features such as quality of service, scalability, mobility and security. Trust is assign to each and every node considering the residual energy and the nodes are secured for a specific time with a time limit. Cluster head node will examine the trustworthiness of the legal and malicious nodes, provides service to trusted nodes and guarantees the expert data exchange. Cluster head defends the data exchange by permitting the trusted entities to take part in the network, separating from the malicious nodes. Trust offers a trust value for each node in a specific way. Fuzzy Logic ensures secure communication between the nodes. Therefore, Trust and Fuzzy logic based technique is an integrated approach which benefits the network with high security, quality of service and the message integrity.

REFERENCES

[1] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinoum, "Sensor Network Security: A Survey", *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52-73 Jun. 2009.

[2] J. Lee et al., "Key management issues in wireless sensor networks: Current proposals and future developments," *IEEE Wireless Commun*., vol. 14, no. 5, pp. 76–84, Oct. 2007.

[3] K. Leena Begum, D. Arun Kumar Reddy, "Design and Accomplishment of TARF: A Trust-Aware Routing Framework for WSNs", *International Journal of P2P Network Trends and Technology (IJPTT)*, vol.11, pp. 20-25, Sep. 2014.

[4] V. Mareeswari, K. Ramakrishna and R. Vijayan, "Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic", *International Journal of Research and Reviews in Computer Science (IJRRCS)*, vol. 2, no. 3,pp. 647-652 , Jun. 2011.

[5] V. J. Sivanagappa, M. Sarumathi, R. Sivaranjani, N. Soniya, "Slip Ring Induction Motor Power Factor Control Using Fuzzy Logic Controller", *International Journal of P2P Network Trends and Technology (IJPTT*), vol. 7,pp. 40-46, Apr. 2014.

[6] S. B. Shaik, R. Arnab, and K. N. Mrinal, "A Direct Trust Dependent Link State Routing Protocol Using Route Trusts for WSNs (DTLSRP)", *Scientific Research on Wireless Sensor Network*, vol. .3, pp. 125-134, Apr. 2011.

[7] R. Vijayan, S. Sumitkumar, "A Novel Approach for Providing Security in Vehicular Adhoc Network through Vehicles Present in the Network", *International Journal of Advanced Research in Computer Science*, vol. 2, no.1,pp. 595-598, Jan. 2011.

[8] I. Farruh, S. M. Aamir, W. K. Sung, and B. Bahodir, "Trust management system in wireless sensor networks: design considerations and research challenges", *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107-130, Jun. 2013.

[9] R. P. Nachiketh , R. Srivaths, R. Anand, N. K. Jha, (2006) , "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols*", IEEE Transactions On Mobile Computing*, vol.5, no. 2, pp.128-143, Feb. 2006.

[10] G.S. Mamatha, and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETS, "*International Journal of Computer Theory and Engineering, v*ol. 2, no. 5, pp. 1793-8201, Oct. 2010.

[11] A.Rajaram and Dr.S.Palaniswami , (2010), "Detecting Malicious Node in MANET using trust based Cross-Layer Security Protocol", *International Journal of Computer Science and Information Technologies*, vol. 1, no. 2, pp. 130-137,May. 2010.

[12] V. Geetha and K. Chandrasekaran, (2014), "A Distributed Trust Based Secure Communication Framework for Wireless Sensor Network", *Scientific Research Publishing Inc*, vol. 6, pp. 173-183, Sept. 2014.

[13] M. Mohit, K. Namarta, N. Esh, and P. S. Aman, "Rule Based Technique detecting Security attack for Wireless Sensor network using fuzzy logic", *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 1, no. 4, pp. 244-251, Jun.2012.

[14] C. Mala, S. Siddhartha, P. Shishir, G. Nagamaputhur, and S. Balasubramanian, "Routing for Wireless Mesh Networks with Multiple Constraints Using Fuzzy Logic", *The International Arab Journal of Information Technology*, vol. 9, no. 1, Jan. 2012.

[15] R. A. Shalikh., H. Jameel, B. J. d'Auriol., Heejo Lee, Sungyoung Lee, and Young-Jae Song , (2009), "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems*, vol. 2, no. 1, pp. 1698–1712, Nov. 2209.