

Full Length Research Paper

Expert security system in wireless sensor networks based on fuzzy discussion multi-agent systems

Shahaboddin Shamshirband^{1*}, Samira Kalantari², Zeinab sam Daliri³ and Liang Shing Ng⁴

¹Young Research Club, Islamic Azad University, Chalous Branch, Iran.

²Young Research Club, Iran.

³Islamic Azad University Chalous Branch, Iran.

⁴Department of Artificial Intelligence Faculty of Computer Science and Information Technology, Malaysia.

Accepted 24 November, 2010

Today, the most basic question concerning wireless sensor networks is designing a system that guarantees their security. One of the issues which has attracted extensive debate is developing a routing process which has the shortest distance and which uses the least amount of power so as the life span of the network can be increased. In this article we intend to create security in the network and also incorporate these two parameters. Therefore, by dividing the network in to clusters and by assigning the head cluster as the master agent, and through negotiations carried out between this agent and the other agents present in the network which function on the basis of multi-agent systems, and by making use of fuzzy decisions made by the master agent, we will deal with how much a node can trust other nodes; and finally, the enemy is identified when it passes through the expert system. Results obtained suggest that this system establishes a high level of security in the network.

Key words: Fuzzy system, multi-agent system, node trust, wireless sensor network.

INTRODUCTION

Wireless sensor networks (WSN) are a subset of AD-HOC networks; therefore, routing in these networks is like that performed in AD-HOC networks (Kuorilehto and Hamalainen, 2005). Generally, the routing algorithm in these networks, as can be seen in Figure 1, is divided into two sections which are the hierarchical and the flat sections.

In flat routing, either the routing table must be updated, or the route must be discovered when requested. In this type of routing algorithm, all nodes function in the same way; that is, they are of equal value from the managerial point of view. Due to difficulties faced in flat routing and because of its inflexibility, the hierarchical routing method was developed in which the network is divided into clusters. In hierarchical routing, group heads carry the main burden of responsibility and the exchange of routing information is carried out among group heads or between a group head and members of the group, and this will

lead to an increase in the efficiency and in the stability of the network (Gerla and Tsai, 1995). The group head, or the cluster head, due to the responsibilities it has, uses a lot of power, and because of this, the cluster head must be changed in order to prevent a reduction in the life span of the network (Yan et al., 2008). One of the methods under consideration for this purpose is to take the residual energy of the candidate node, the number of neighbors, and the number of the cluster heads which are in the vicinity of the neighbors into consideration. In this way the power to be consumed is divided among nodes; and in the end the life span of the network will increase (Ansari, 2008).

In some cases, the value of each node is taken in to account in order to choose a manager node, or a node which manages a number of sensors. In Basnet and Mukkamala, (2009), the value of each node is in the form of the temperature, the smoke, and the light which are present in the environment and which are measured by the node. The values are compared and the node which has the highest value is chosen as the manager node. The activities of the manager node have an important

*Corresponding author. E-mail: Shamshirband@iauc.ac.ir.

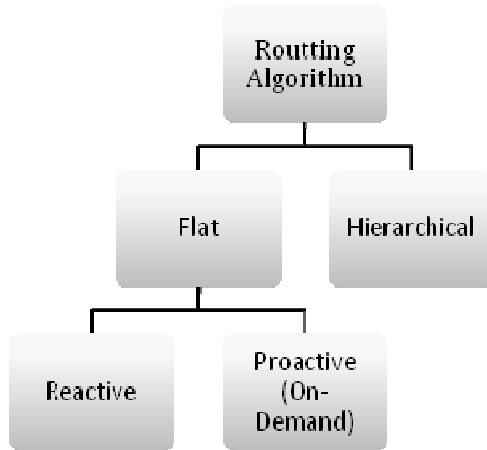


Figure 1. Routing algorithm in dynamic networks.

role in the life of the network. For example, with the failure of a node in the distributed network the whole network may fail because the nodes are dependent on each other. In Majma and Pedram, (2008) the dynamic immigration process is dealt with in connection with confronting failure in distributed systems. In this process, the data stream immigrates to a node which has the suitable conditions. These suitable conditions refer to the average workload of the node, that is, the node which has a lighter workload is chosen by the manager and will be in charge of continuing the process.

The EESR routing which has been improved by the fuzzy inference system in a wireless sensor network (Taheri and Movaghar, 2008) is a project in which the parameters of distance, and the link used are taken into consideration in order to optimize the routing process. In this network the node for transmitting information packages is chosen by fuzzy logic with the purpose of increasing the life span of the implemented network.

In the literature on security, the two terms “threat” and “attack” are more or less used to refer to the same concept, while “threat” is a potential danger that creates vulnerability and “attack” is an assault which ensues from a smart threat. Attacks on security are divided into active and passive attacks. Passive attacks do not affect resources, which active attacks can influence resources, change data, and facilitate or restrict access to data. Active attacks include changing the message, forging the message, etc (Stallings, 2005). Attacks are waged in an attempt to breach the security features of networks (Stefano et al., 2007).

Wireless sensor networks, like wireless networks are often exposed to threats and attacks leading to the instability of the networks. However, the difference between wireless networks and WSNs is that in WSNs there are nodes and sensors which are both numerous and mobile; and this dynamism will result in an irregular structure. There is also this possibility that under certain

conditions nodes are injected into the network and, when this happens, the position of the network is in jeopardy and discussion of network security becomes necessary. Some of the attacks waged against wireless sensor networks are as follows (Cole, 2005; Saraogi, 2004): Passive information gathering, false node and malicious data, subversion of a node, Sybil Attack, Sinkhole Attack, Wormholes, etc.

Security in cooperative communications is a significant concept. In Makda (2008) a project is put forward in which a helper node is used to increase the speed of transmitting data between the source and the destination nodes. Use of this node creates security problems, and two projects (WAP, WAP2) have been proposed to establish security in cooperative environments.

Attacks on networks are often in the form of using various addresses in IP and various personal characteristics in different time intervals. That is way it is difficult to recognize enemies (Kazemeyni, 2008).

Jin (2007) presents negotiation framework based on agent theory to support collaborative design decision-making. Agent Based Negotiation framework (ANF) is composed of a negotiation protocol, a set of negotiation strategies, and a network of intelligent agents. This method was implemented to a layout designed for machine. Negotiation strategies and tactics together determine the direction of negotiation: whether to explore the value space of current issue, or identify new issues at the same level, or to move to a higher level or relevant issues. Each strategy is composed of a set of IF-THEN rules with tendency of moving negotiation to a specific direction.

Host information or network information can be used to identify enemies in passive attacks on WSN. Passive attacks include overhearing and supervision of data transmission. It is very difficult to detect such attacks because they do not cause any changes in data (Stallings, 2005). Kyung (2008) method has been proposed to detect worms in P2P networks; and since worms do not cause general changes in the network, this is a host-based method. Worms have to communication with their victims to be able to wreck networks. In this method, by checking the number of communications and the time intervals between them, it becomes possible to suspect presence of worm –that is with an increase in the number of host communications the time intervals between these communications decrease and, if the given event is infected and the nodes are safe, Baire’s probability is used for investigation; and finally it is announced whether the node is safe or a warning is issued that there is a danger of infection.

In Daneshfar (2009), the degree of safety of each node is calculated to establish safe communications in wireless sensor networks. In this system T stands for Trust and U represents Distrust, and the ranges are assumed to be $U < 1$ and $T > 0$. And U is determined by using formulas 1 and 2:

$$T = \frac{Avg(T_i, T_j)}{1 - (Avg(T_i, U_j) + Avg(T_j, U_i))} \quad (1)$$

$$U = \frac{Avg(U_i, U_j)}{1 - (Avg(T_i, U_j) + Avg(T_j, U_i))} \quad (2)$$

VANET (Vehicular Ad-Hoc Networks) is a type of MANET and resembles wireless sensor networks, with this difference that its nodes and sensors are vehicles. The main purpose in this network is to improve vehicle and driver safety through communications among vehicles. These networks, like wireless sensor networks, are also very vulnerable to attacks. Sybil attack is an example of these attacks, and it has been designed with the aim of making the VANET throughput vulnerable. The malicious node presents itself as a safe node, causes traffic in the network through introducing incorrect information, and plunders the network (Wooldridge, 2009).

A method has been proposed for VANET (communication of verification sensor) in which the degree of security and the trust values of the nodes which are immediate neighbors are determined through mathematical calculations to be between (-1) and (1). Other methods have also been suggested in which it has been attempted to find a way to keep networks secure from attacks. Some of these methods are: Autonomous Sensor, ART (Acceptance Range Threshold), Maximum Density Threshold, MGT (Mobility Grade Threshold), Cooperative Sensors, Overhearing.

In the final analysis, what seem to be necessary in these networks are the identification and the destruction of the enemy. In this article, we have tried to use cooperation among agents present in the network, and we have employed fuzzy logic to identify suspicious and destructive nodes.

The article is organized as follows: multi-agent systems are defined in part two, and fuzzy systems in part three. In part four our proposed security system is explained. Part five deals with simulation, and conclusions and future research are presented in part six.

MULTI-AGENT SYSTEM

A multi-agent system (MAS) consists of a set of agents, each of which is independent and autonomous. These agents communicate among themselves and function in a cooperative and coordinated way to reach the general and common goal. Agents are software programs which include predetermined characteristics and feature. In these systems, the agents must communicate with each other and function in a coordinated way. Each agent of such a system uses a control algorithm, and when it deems necessary (in other words, when it wants), it can communicate with other agents (Daneshfar, 2009; Zadeh, 1965). The architecture of such a system is shown in

Figure 2.

In multi-agent systems the complexity of the system and the software costs are reduced because the workload is distributed, information is collected in a common work environment, and the processes of decision making and achievement of the goals can be carried out faster (Sarnecki and Kraus, 2005).

It is inferred from the above definitions that we can employ agents that are somehow smart to design systems that cannot be created by using single-agent systems. It is for this very reason that smart multi-agent systems have enjoyed widespread applications. MASs is the most suitable method to achieve the goals in distributed systems (Daneshfar, 2009).

In our proposed system every node is recognized as an agent, which has the ability to make decisions. Agents function both individually and collectively; that is each agent individually collects its own information and that of its specific environment and processes this information, if necessary, asked by the network, provides this information for some other agents. These agents enjoy difference in the network so that some of them play more important roles (such as the master node in Figure 3), and the other agents must obey these more important agents.

FUZZY SYSTEMS

References to cited sources should be incorporated within the text (Gerla and Tsai, 1995). Bibliographical references must be placed at the end of the paper and comply with the model below. Professor Lotfi Zadeh is one of the best-known names in modern mathematics. He first introduced the theory of fuzzy sets and fuzzy logic in 1977 when he wrote his first article entitled Fuzzy Set. His goal was to develop a model describing processing in natural languages (Zadeh, 1967).

Fuzzy logic, which formulates qualitative parameters, is a continuous logic in which the model of approximate reasoning of human beings is used. In Boolean logic, 0 and 1 (correct and incorrect) are accepted- and this is the same logic used in computers. However, in Fuzzy logic an attempt is made to determine approximate figures (for example, figures between zero and one); and in fuzzy logic the trust value is not restricted to zero and one, rather it can be an interval between zero and one. Fuzzy logic is applied in recognizing the domain of continuous variables, and it is a technology which controls those non-linear and multi-parameter systems which are difficult to prove by using mathematical rules. Moreover, the solution offered by fuzzy logic is much faster than the design techniques of control rules. This system is based on knowledge, and rules present in the knowledge base are used in decision making (Yan et al., 2000). Figure 4 shows the general structure of a fuzzy system.

The advantages of using fuzzy logic in control systems are as follows: the ease of applying the IF...THEN...,



Figure 2. Architecture of multi-agent systems.

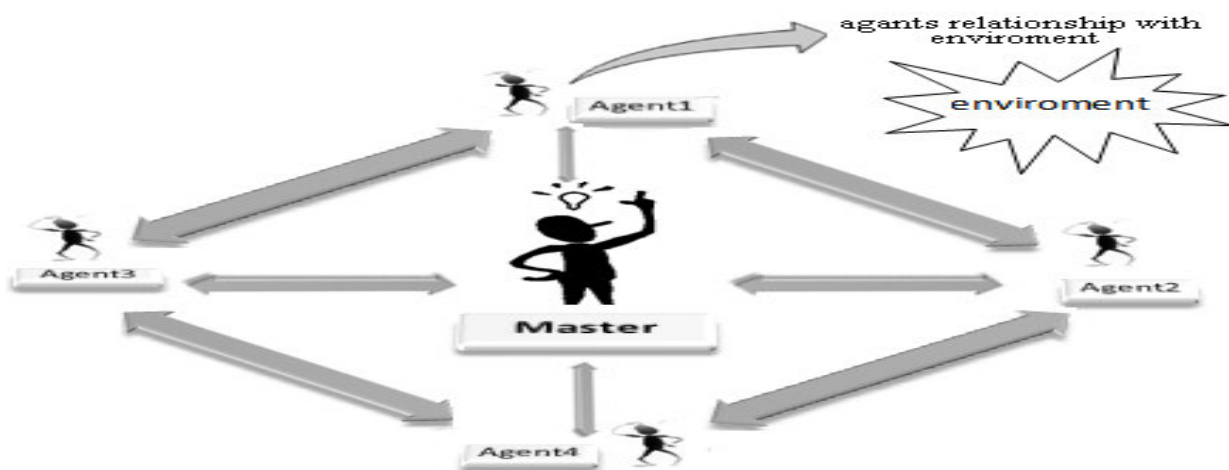


Figure 3. A representation of the relations between the Master agent and the other agents present in the network.

rules instead of using difficult expert rules, the understand ability of fuzzy logic for people without background in control processes, and the availability and readability of software and hardware tools which use fuzzy logic as an applied technology (Robert and Isimhemem, 2009).

In our proposed system fuzzy logic is used to assign trust values for nodes. Consequently, it is not merely a question of trust or distrust in a node, but rather different trust values can also be considered. For example, in the interval $[-1, 1]$, which is assigned to represent the degree of trust $[0.5, 1]$ shows complete trust and $[-0.5, 0.5]$ indicates approximate trust in the node. With such an approach, the nodes present in this system know how far they can trust or be suspicious of other agents (as can be seen in Figure 5) in order to keep themselves from enemy attacks.

OUR PROPOSED METHOD OF ESTABLISHING SECURITY

Due to the characteristics of wireless sensor networks that was explained in part one, they provide a good opportunity for attacks and for their penetration into the network. In these networks there is insecurity and distrust not only in packages sent (input) but also in the nodes (agents) present in the network. This means that both the data and the nodes present in the network must be secure. With the point of view that data become somewhat secure by following rules of encryption, this project was undertaken with the purpose of establishing security in the nodes or agents present in the network. So that, through giving titles of trust (secure, reliable) and distrust and by identifying destructive nodes, the host nodes present in the network can make a more suitable decision concerning the nodes they want to interact with

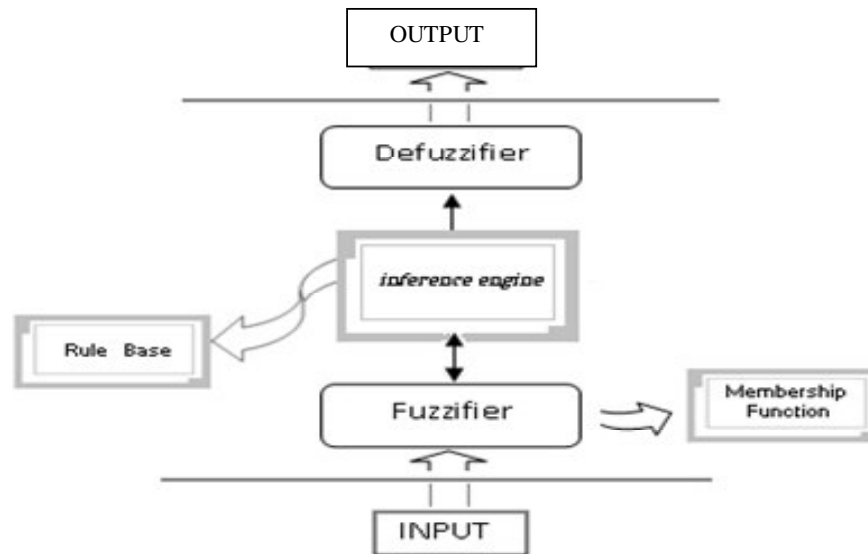


Figure 4. The structure of a fuzzy system.

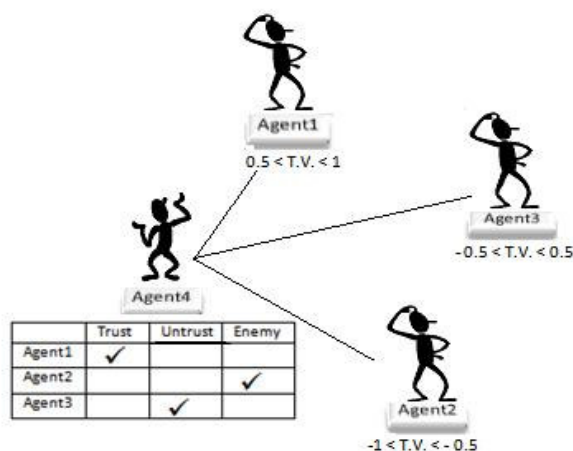


Figure 5. Identification of agents which cannot be trusted.

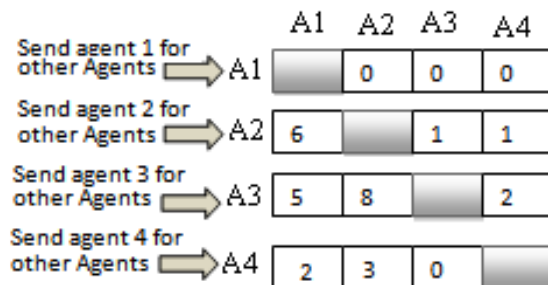


Figure 6. Communication of an agent with other agents in the array.

node belonging to the network or a destructive node.


In this project, the network is divided into clusters and each cluster is guided by a cluster head. In order to prevent a reduction in the life span of the network due to the increased workload of the cluster head, this node is replaced with another node, which meets the necessary requirements for becoming a cluster head, at a specific time interval (Δt) so that nodes can enjoy a balanced state as far as their power level is concerned (Ansari, 2008).

Every node in the network is considered an agent which dynamically communicates with the other agents and with the cluster head named Master. This forms the basis of multi-agent systems. The Master must obtain information from the network, which is information gathered by the other agents present in the network (Figure 3).

In this method, features have been added to the agents and to the cluster head so that every agent present in the network has the memory in which it saves information. As can be seen in Figure 6, this information (hypothetical numbers in a hypothetical system) consists of an array from which the numbers of messages sent from the node to other nodes, and received by the node from other nodes, are derived. The Master table contains general information present in the cluster and in the network, together with a tabular array which keeps in itself information concerning messages sent and received by all the nodes present in the network (Figure 7).

After the time interval (Δt), the Master node quarries the cluster. In this quarry, which is carried out between the Master and the other agents present in the cluster, the Master table is completed (when the Master is changed, this table is transmitted to the new Master and is deleted from the old Master. This is done to provide security to

and so that the host nodes may know whether the node sending or receiving the package is the same authorized



	Agent1	Agent2	Agent3	Agent4
Send	0	8	15	5
Receive	15	11	1	3

Figure 7. The Master table

Table 1. Fuzzy linguistic variables in the control system.

Parameter	Type	Linguistic variable
input	Send	Low, medium, high
input	Receive	Low, medium, high
output	Trust value	Trust, distrust, enemy

Table 2. Classification of fuzzy rules in a security system of trust in agents.

		Receive		
		Low	Medium	High
Send	Low	trust	distrust	Enemy
	Medium	distrust	trust	Distrust
	High	enemy	distrust	Distrust

this node against possible attacks and in order to obtain information contained in the cluster head). From this moment on, the Master uses its inbuilt expert system and the information obtained from the network (from the Master table) to prove the authenticity of the nodes present in the network and to identify these nodes.

Generally, the expert system includes two parts which are the knowledge base and the inference engine. The inference engine processes knowledge and draws conclusions on the basis of the present information and the knowledge saved in the knowledge base. The knowledge base in the system under consideration includes two categories of information: the first category contains information through the use of which, and by employing fuzzy logic, the inference engine deals with the trust values of the nodes present in the network. The second category includes codes. Each of the agents is assigned a unique code.

Assuming that the time interval Δt is ten seconds and the maximum number of transmissions during this time interval is 15, we will now deal with the fuzzy control system we have in mind.

The input parameters of the fuzzy system are derived from the table present in the Master. These parameters

are the number of messages sent and received.

Input: Send (0...5) (5...10) (10...15)

Receive (0...5) (5...10) (10...15)

Output: Trust Value (-1, -0.5) (-0.5, 0.5) (0.5, 1)

By classifying the input parameters according to Table 1, and the output Trust Value into Trust interval (-1, -0.5), Distrust interval (-0.5, 0.5), and Enemy interval (0.5, 1), we will have the following fuzzy structure.

The fuzzy system used in the inference engine of the expert system is the Mamdani fuzzy system. The Mamdani fuzzy system is a simple rule-based method which does not require complicated calculations and which can employ the IF...THEN... rules to control systems. Mamdani was the person who used the fuzzy method for the first time to study the process of controlling steam machine. Since then, this method has been in use and has acquired a special status.

The input data (Table 1) enter the fuzzy system and the fuzzy inference (the Mamdani inference) is employed to produce the desired output. This inference is derived from asset of rules which are inbuilt in the fuzzy system.

Taking into account intervals of the input and output parameters above and the fuzzy inference in Table 2 (the general format of fuzzy rules), the states agents present in the hypothetical system are identified as follows:

This system has been implemented in the fuzzy toolbox of subject software. The input and output membership functions of this security system are shown in Figures 9 and 10; and the surface diagram in Figures 8 and 11 shows the Trust Values of nodes regarding packages sent and received.

In the end, the suspicions node passes through the inference engine of the expert system so that its authenticity can be proved. The node suspected of being an enemy is responsible for answering a code (each node has a unique code and no agent other than Master has access to these codes).

The agent who is the member of the network must be able to answer the code (like a key by which an agent is identified and receives the label of Trust). The central station can assign and update the codes and inform the nodes and the Master of the codes. This information requires encryption algorithms that can use private and public keys. Of course, it is worth noting that the use of keys entails effects such as reduction in speed (Wooldrige, 2009; Ertaul and Ganta, 2009; Ertaul, 2009; Eronen and Zitting, 2001). For this very reason, this method is only used for nodes that cannot be trusted (Figures 12 and 13).

If the expert system receives the correct answer from the agent, it will consider the agent safe; otherwise, the agent will be identified as enemy and the Master agent informs the whole network of the presence of the enemy node.

The operations performed in the algorithm are shown in

If Send=Low and Receive=Low then Station=Trust A4
 If Send=Low and Receive=Medium then Station=Distrust
 If Send=Low and Receive=High then Station=Enemy A1
 If Send=Medium and Receive=Low then Station=Distrust
 If Send=Medium and Receive=Medium then Station=Trust
 If Send=Medium and Receive=High then Station=Distrust A2
 If Send=High and Receive=Low then Station=Enemy A3
 If Send=High and Receive=Medium then Station=Distrust
 If Send=High and Receive=High then Station=Distrust

Figure 8. The general format of fuzzy rules.

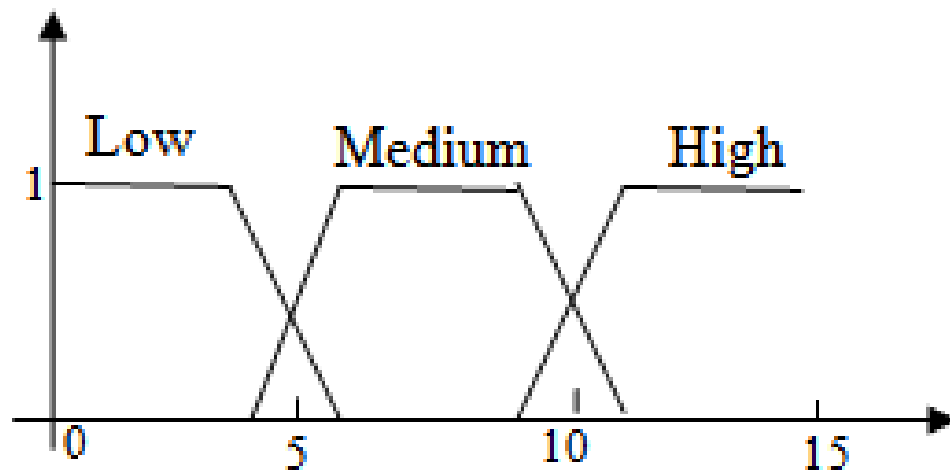


Figure 9. The membership function of input parameters sent and received

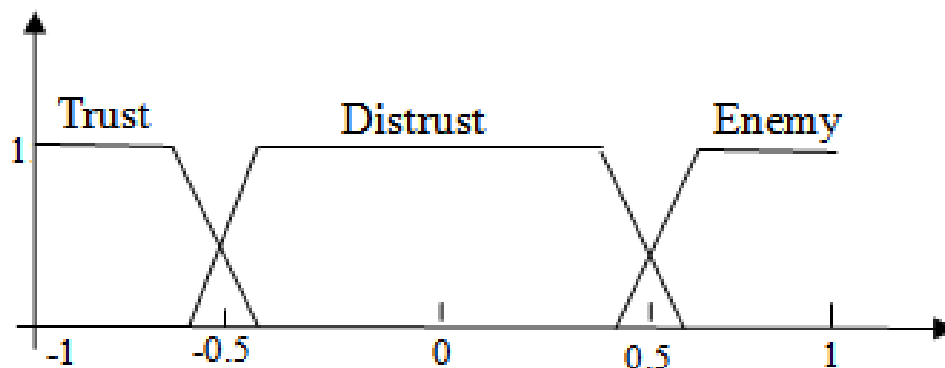


Figure 10. Membership function of output trust value.

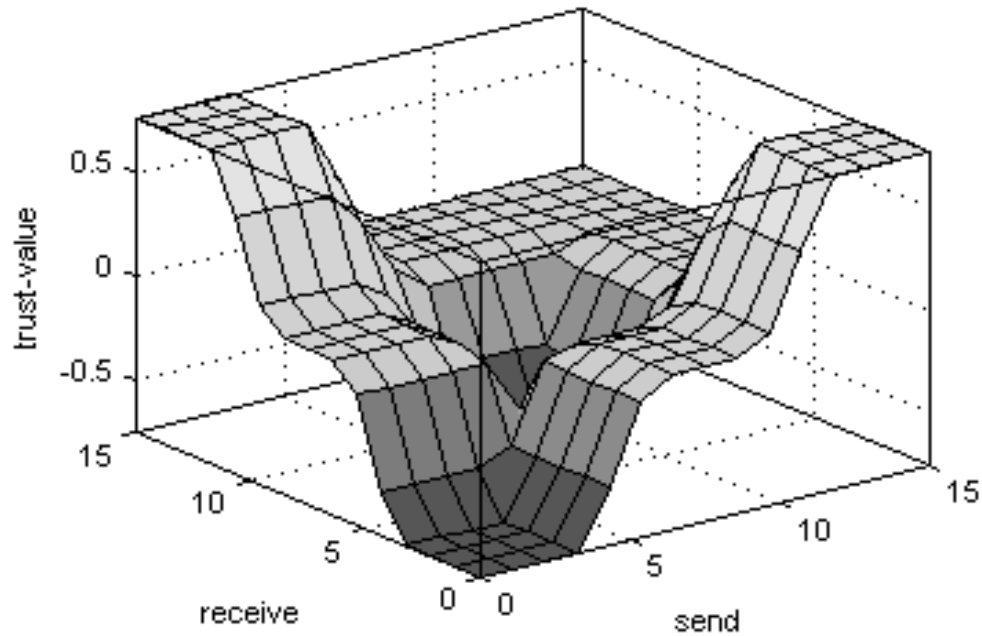


Figure 11. Trust Value of the nodes present in the network.

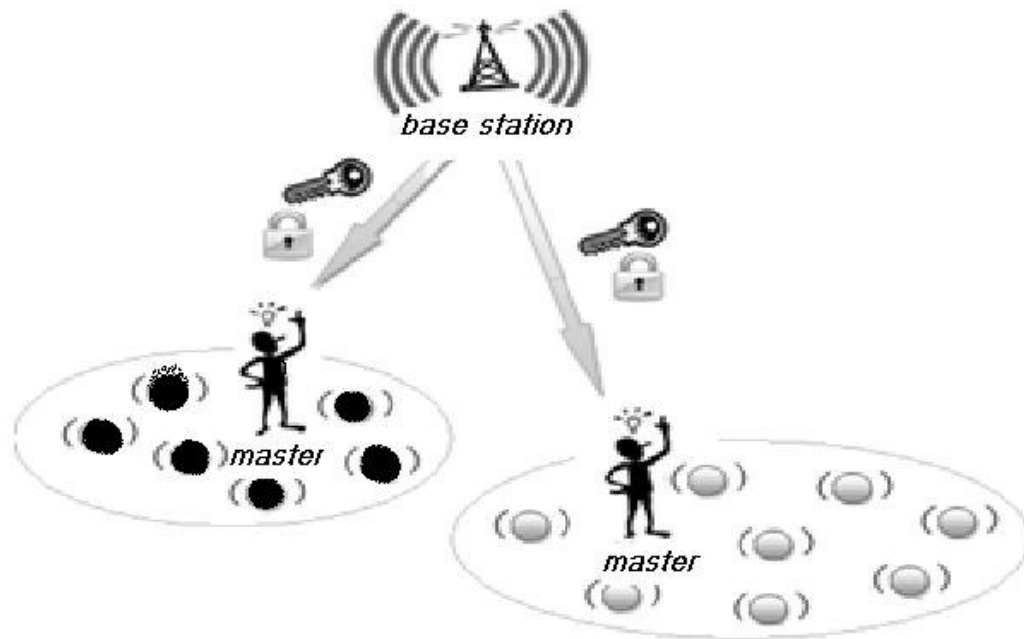


Figure 12. The relationship between Master and the bus station and identification of agents which are members of the network.

Figure 14. There are two phases of decision making: one for determining the trust values of nodes and the other for identifying enemy agents and for differentiating agents which can be trusted from those which must be distrusted. In this system, according to the algorithm, quarry from the cluster is carried out by the Master agent; and the Master table is formed according to the number

of sent and received messages. This table functions as the input of the expert system. The fuzzy control system, and the system for identifying agents which cannot be trusted, form the inference engine of the smart expert system. The inference engine recalls the required data from the knowledge base of the expert system—that is, the fuzzy system uses the information in the Master table,

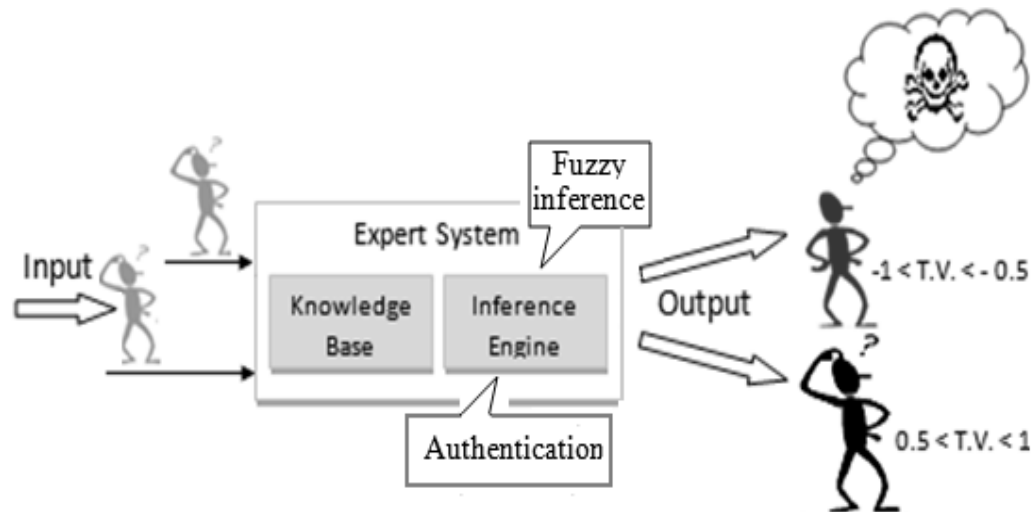


Figure 13. The performance of the expert system in the proposed method.

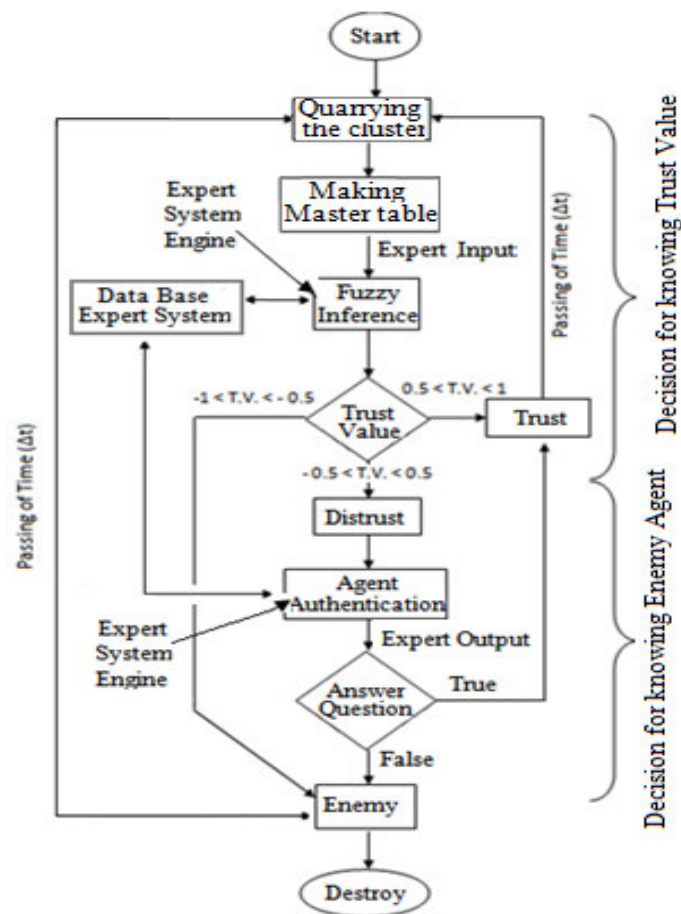


Figure 14. The operations of the algorithm.

and matches this information with that of the knowledge base, to identify the three domains of Trust, Distrust, and

Enemy. The first and the third domains form the output of the expert system provided the identity of the agent that

cannot be trusted for transmitting information which has not been established. For this very reason, the authenticity of this agent is investigated by using the unique codes given to the agents in the knowledge base of the Master expert system. If the Master recognizes this the agent is identified as an enemy.

Some of the attacks made on wireless sensor networks are Gray hole, Wormhole Attack, Sinkhole Attack, Rushing, etc. In these attacks the destructive node tries to decrease the power of the network through sending a false package, or it uses repetitive information and repeatedly sends it. Another possibility is that the destructive node claims to be a safe node, causes traffic in the network, and in the end discards all the packages that are sent to it. Our proposed system is quite able to recognize these attacks and to identify the destructive node.

Conclusions and future research

This article has dealt with designing a system that can differentiate agents that can be trusted from those that cannot be trusted on the basis of fuzzy negotiations among agents present in the network. The purpose has been to establish security in wireless sensor networks. In the end, the expert system identifies the enemy and informs the network of its presence. In this way, in the operation of transmitting packages, the host nodes present in the network can make appropriate decisions concerning the node to which information package must Be sent or from which the information package must be received; and these host nodes can also learn if the node in question is a member of the group or not.

In our future research, we intend to use cooperation among agents present in the network to destroy the destructive node or agent and remove it from the network.

REFERENCES

- Ansari A (2008). Grouping in Ad hoc network for energy consuming and increase life cycle networks, 16 Iranian conferences on Electrical Engineering, May 13-15.
- Basnet R, Mukkamala S (2009). Event Detection and Localization using Sensor Networks, ICWN'09: July 14.
- Cole E (2005). Network Security Bible, published by John Wiley & sons.
- Daneshfar F, Hassan B (2009). Multi -Agent Systems in Control Engineering: A Survey, J. Control Sci. Eng., Article ID 531080, 12 p. doi:10.1155/2009/531080.
- Eronen P, Zitting J (2001). An Expert System for Analyzing Firewall Rules", Proc. Sixth Nordic Workshop Secure IT Systems (NordSec'01), pp. 100-107.
- Ertaul L, Ganta M (2009). Security in Wireless Sensor Networks—A Study .Proceedings of the 2009 International Conference on Wireless Networks, ICWN 2009, July 13-16.
- Ertaul SM (2009).The Security Problems of Vehicular Ad Hoc Networks (VANETs) and Proposed Solutions in Securing their Operations. The 2009 International Conference on Wireless Networks ICWN'09, July, Las Vegas.
- Gerla M, Tsai JTC (1995). Multi cluster, Mobile, Multimedia Radio Network, in ACM Baltzer J. Wireless Networks, 1(3): 255-265.
- Jin Y (2007). Agent Based Negotiation for Collaborative Design Decision Making, CIRP Annals - Manufacturing Technology, 53(1): 121-124.
- Kazemeyni F (2008). Detection based on P2P worm. 16 Iranian conference on Electrical Engineering.
- Kuorilehto M, Hamalainen TD (2005). A Survey of Application Distribution Wireless Sensor Network, EURASIP J. Wireless Commun. Networking, 5: 774-788.
- Majma M, Pedram H (2008). Dynamic Immigration process for fault detection in distributed computing systems process, 16 Iranian conferences on Electrical Engineering, May 13-15.
- Makda S, Choudhary A (2008). Security Implications of Cooperative Communications in Wireless Network, Sarnoff.Doi10.1109/SARNOF.2008.4520069.
- Robert OE, Isimhem O (2009). Design of Cryptographic Software for Wireless Network Security, Security and Management, pp. 166-169: Las Vegas, Nevada, USA.
- Saraogi M (2004). Security in Wireless Sensor Network, ACM SenSys., pp. 330-339..
- Sarne D, Kraus S (2005). Cooperative Exploration in the Electronic Marketplace", American Association for Artificial Intelligence, In Proc. of AAAI.
- Stallings W (2005). Cryptography and Network Security Principles and Practices, Fourth Edition, Publisher: Prentice Hall, Pub Date: November 16.
- Stefano B, Alessio C, Emanuel M (2007). Controlled sink mobility for prolonging wireless sensor networks. Lifetime, 14(6): 831-858, ISSN 1022-0038.
- Taheri N, Movaghar A (2008). Performance of EESR routing based on fuzzy system in wireless sensor networks". 16 Iranian conference on Electrical Engineering, May 13-15.
- Wooldridge M (2009). An Introduction to Multi agent Systems. Second edition by John Wiley & Sons. Published May .ISBN-10: 0470519460.
- Yan XW, Deng ZD, Sun ZQ (2008). The Adaptive Cluster Head Selection in Wireless Sensor Networks, Semantic Computing and Applications.
- Yan XW, Deng ZD, Sun ZQ (2000). Fuzzy Advantage Learning. Fuzzy Systems, 2000. FUZZ IEEE 2000. The Ninth IEEE International Conference.Doi 10.1109/FUZZY.2000.839145.
- Zadeh LA (1965). Fuzzy Sets. Inform. Contr., 8: 338-353.