Research Journal of Applied Sciences, Engineering and Technology 10(10): 1175-1184, 2015 DOI: 10.19026/rjaset.10.1885
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: February 22, 2015 Accepted: March 12, 2015 Published: August 05, 2015

Research Article

An Improved Role Based Trust Management System using Interactive Artificial Bee Colony (I-ABC) Algorithm for Wireless Sensor Networks

[1]K. Vignesh and [2]N. Radhika,
[1]Manonmaniam Sundaranar University, Tirunelveli, India
[2]Department of Computer Science Engineering, Amrita Vishwa Vidhya Peetham, Coimbatore, Tamilnadu, India

Abstract: The aim of this research study is to propose an improved role based trust management system for wireless sensor networks. The objective is attained using an interactive artificial bee colony algorithm which is used for path optimization. Also the purpose is to guarantee to provide robust and trustworthiness among the clusters formed in the wireless sensor network. The reputation among the sensor nodes is assured using the trust model. One of the main concerns of WSN, that have attracted research scholars, is the property to guarantee a less amount of security in a limited environment. Trust among the communicative nodes is one of the major issues that have to be given importance in wireless sensor network. A number of research works have concentrated on only Trust Management (TM) techniques without considering their roles. Existing trust management schemes do not provide significant reliability in all environments. In order to overcome these issues, Role Trust (RT) framework is presented, to select role for each nodes representing policies in a distributed authorized environment. RT integrates the features of role-based access control and TM schemes. This feature is particularly applicable for attribute based access control. Role trust management schemes generate rules, identify and assure roles based on the rules generation process and then clusters are identified for each trust model. Along with the trust model, this study focuses on efficient data path with reduced data loss. Hence, this study presents a novel Swarm Intelligence based Role Trust and Reputation Model (SIRTRM) to provide trust and reputation in WSNs. Simulations are carried out in NS2 environment and the results portrays the accuracy, robustness and lightness of the proposed model.

Keywords: Artificial Bee Colony (ABC), cluster, reliability, Role Based Trust Management (RBTM), Trust Management (TM), Wireless Sensor Networks (WSN)

INTRODUCTION

WSNs consist of several spatially distributed components that observe and transmit the aggregated data to a position in middle with the help of wireless channels. Since restricted resource facilities of WSN, it is not an easy task for integrating fundamental security model such as authentication, reliability and key distribution. Since WSN have several interesting science and engineering applications, a number of research works have been carried out to develop efficient security schemes. But, most of the WSNs consist of nodes with highly dynamic topology which may results in certain scalability issues.

As a result, WSN are susceptible to various types of malicious attacks, such as denial of service, routing protocol attacks as well as replay attacks. Conventional crypto schemes are insignificant in handling such malicious attacks. Thus, trust and security management schemes have become an attractive research area in WSN (Aivaloglou *et al*., 2006). However, conventional trust management approaches may not be appropriate for networks with small sensor nodes due to restricted bandwidth and rigorous node constraints in terms of power and memory (Ganeriwal and Srivastava, 2004; Yao *et al*., 2006). Moreover, it is observed from the literature that certain techniques do not consider the dynamic factors of trust (Shaikh *et al*., 2009) which results in insignificant performance of dynamic topology.

Another major issue in WSN is that nodes could misbehave when certain data are extracted from them. Conversely, the sensor nodes are usually fixed in environment where there is a possibility of an intruder are able to capture them along with consequently use these nodes to attack the whole network (Ren *et al*., 2003). Therefore, it is necessary to recognize the compromised nodes and eliminate them from the network so as to prevent the whole network from the intruders.

This research study aims to develop a more suitable role based efficient trust model for WSN in order to enable mobile sensor nodes to exchange trust opinions with minimal overheads. To represent policies

Corresponding Author: K. Vignesh, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India

for each node such as either cluster head or cluster member and credentials in distributed authorization. Development of the RT framework is the main effort to address security issues that arises when independent organizations enter into coalitions and for system whose membership and existence change rapidly.

In general, client server architecture depicts some nodes of the network request some services and others provide those services. Sometimes a node could provide a fake service for triggered request. In order to avoid such situation, this research work uses the best path selection based on swarm intelligence approach. Swarm Intelligence based Role Trust and Reputation Model (SIRTRM) is proposed in this research for the selection of the most trustworthy node based on the reputable path selection offering a certain service. The swarm intelligence used in this approach is Artificial Bee Colony (ABC) Algorithm.

LITERATURE REVIEW

Security considerations in WSN have increased in the last two decades mainly due to its applications in various military related applications. Trust based management system have increased to overcome the problem of security level in WSN (Ferraiolo *et al*., 2001). Most of the earlier trust management systems do not consider trust level for individual nodes in the network along with roles. For example, a multi path routing protocol based on dynamic clustering methods and ACO, is described in MRP (Yang *et al*., 2010), which enhances better data aggregation with trust, thereby reducing the energy consumption.

Fuzzy and extended fuzzy based trust management methods for WSN have also been proposed for effective management. Zarei *et al*. (2009) proposed a fuzzy logic based framework to control network traffic in WSNs. TFCC protocol is proposed in Chakaborty *et al*. (2013), which controls congestion traffic of network, from source nodes to sink nodes with improved network throughput. Trust based management system for WSN uses a swarm intelligence based methods (Dhurandher *et al*., 2009) to improve reliability and QOS in WSNs. QoS results are estimated based on Quality Distance Vector (QDV) protocol. The result of this shows that the proposed swarm intelligence based protocol have to achieve higher reliability for communication. The above mentioned trust management methods does not assign roles for each nodes in WSN. In such methods, the nodes are randomly chosen as cluster heads. Based on chosen cluster head, remaining nodes are grouped. Thus, there are still spaces for better security schemes. Therefore, the present research work focuses on role assignment to each node in the network using role based languages. RBAC Model (Ferraiolo *et al*., 2001) provides flexibility category of access control procedure. An access control policy group similar user roles and allows users to access the resources of the system. The entire description of role trust language specification for various applications is described in Li and Wang (2007) and Li *et al*. (2003). In this study, based on role trust framework, roles are assigned to nodes in WSN.

METHODOLOGY

Proposed Role Trust Management System (RTMS) and optimal path selection using Artificial Bee Colony (ABC) algorithm: In earlier work, (Marmol and Perez, 2011) developed an efficient trust model framework for WSN based on bio-inspired optimization methods. It follows the procedure of ant colony system based on user requested service in WSN, Where each ant is considered as nodes that receives the right requested service and gets adapted, to find the trust worthiness of a cluster head. The results are carried out to measure accuracy and strength of this trust model. The present research work, trust management system is extension of this model and it is enhanced in several points of view. The existing trust based management system does not consider the roles based on the efficiency of the rules. The proposed system creates a role trust based cluster model in WSN to select roles such as Cluster Head (CH) and Cluster Member (CM) along with the residual energy and trust value for each node. Once the cluster head is elected, then the next process is the formation of clusters based on the Role based Trust with semantic Rules (below section). Based on the semantic rules, the most important trusted node is elected as a cluster head. Which forwards the data to the selected cluster head and also an efficient path selection is done to destination node using ABC without loss of packet. Then, ultimately, the current cluster head energy level is checked with specified threshold value, if less than threshold value then reelection are triggered. The proposed system is shown in Fig. 1.

The basic concepts of roles are analyzed by the role based trust management system model and there by the trust value of each node are computed. In this study, a node to node level trust is considered and it is estimated based on the earlier interaction among nodes in communication. Similarly, trust values are calculated for entire role nodes in role trust management. The procedure is explained below.

Cluster formation: A clustering architecture offers fault tolerance along with network scalability that will give the outcome of exploiting the network resources. Clustering can be applied effectively for resource management, routing and location management and also drastically lessen both communication overhead and computational time complexity.

Cluster head selection: In first phase of the proposed system form a cluster by selecting the cluster head

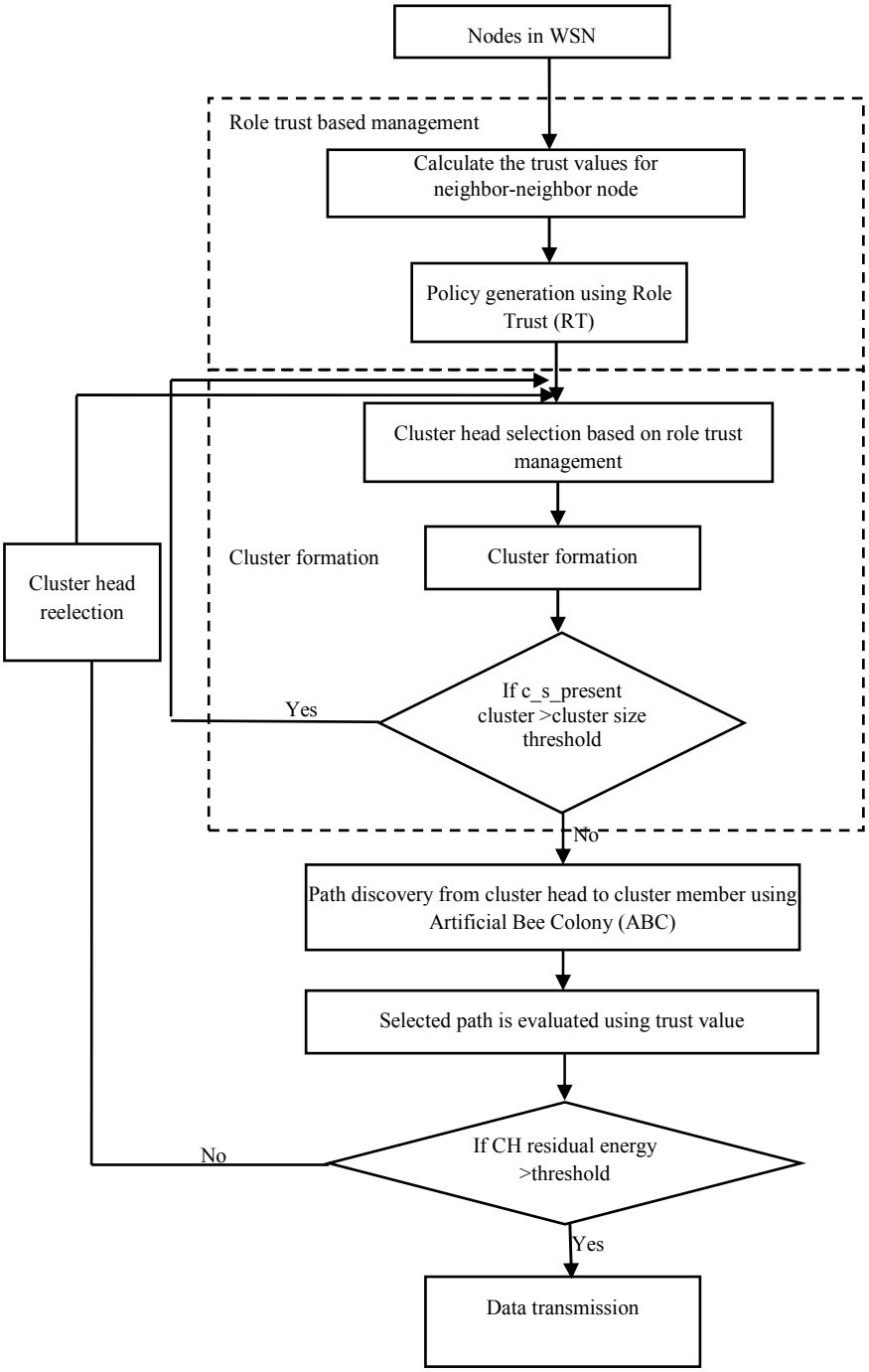

Fig. 1: The proposed architecture for role trust based cluster formation and optimal path selection

among the eligible nodes. The cluster head is selected based on the calculation of trust value, residual energy for each node and based on that calculation it forms roles such as Cluster Head (CH) and Cluster Member (CM). The calculation of the trust values and role formation are given below.

Trust value calculation:

Time based past communication trust evaluation: Node level trust value is estimated based on earlier communication in node level from node y at the location of node x, it is defined as:

$$PC_{x,y} = 1 - \frac{1}{\max[\{w_s SI_{x,y} - w_u UI_{x,y}\},0]+1}$$

where,

$PC_{x,y}$ = The past communication value of node y estimated by node x based upon the past communication

$SC_{x,y}$ = The successful communication value of node x with node y based upon the past communication

$UC_{x,y}$ = The successful communication value of node x with y based upon the past communication at node level

w_s &w_u = Positive numbers with satisfied time and represent the related weights of $SC_{x,y}$ and $U\ C_{x,y}$

The weight value of the communication nodes w_s is defined as:

$$w_s = \begin{cases} h\ t_s = 1 \\ m\ t_s = 2 \\ l\ t_s > 2 \end{cases}$$

Similarly w_u is also defined. This mapping of results improves trust values results based on assigning high, low and medium communication time. The time t_s is defined as:

$$t_s = \left[\frac{T_{current} - ST_{x,y}}{\Delta T}\right] t_u = \left[\frac{T_{current} - UT_{x,y}}{\Delta T}\right]$$

where,

$T_{current}$ = The current time

$ST_{x,y}$ = The time of $UT_{x,y}$ last successful past communication

ΔT = The threshold time

Peer recommendations evaluation: Assume that there is n number of nodes in WSN and every node in WSN has a unique id. When any node gets peer suggestion then it calculates the trust value of each node in the network by using following formula:

$$PR_{x,y} = \frac{\sum_{i=1}^{n-1}[Tv_{x,i} * Tv_{i,y}]}{n-1}$$

where,

$PR_{x,y}$ = The peer recommended trust value of node y calculated by node x

$Tv_{x,i}$ = The trust value of node 'i' calculated by node x

$Tv_{i,y}$ = The trust value of node 'y' calculated by node i

Let's suppose node x wants to calculate the trust value $Tv_{x,y}$ of node y, then it can be evaluated by the following equation:

$$Tv_{x,y} = \frac{(PI_{x,y} + PR_{x,y})}{2}$$

After the trust values are calculated for each node, then the process of creating the clusters by assigning the roles for each node. Clustering is done for each node after the election of cluster head. Then the roles are assigned which alternatively based on the size.

Roles created based on the trust value calculation: In general, role based trust management system follows the procedure of creating roles (Li and Mitchell, 2003), it can be implemented to cloud computing methods to access control of VMs (Lasota and Kozakiewicz, 2012) and trust in WSN. Some conditions are defined to each role in the Wireless sensor networks, for discriminating roles activations. It uses various entities to differentiate roles of each node in WSN. Roles define a set of entity which is a member of either the cluster head or the cluster member. An entity is an association of a cluster head condition and only if all the nodes in the remaining trust values are comparable to the cluster head. In earlier work, ref (Gorla *et al*., 2006) is based on time dependent principles for role trust. A central organizing notion in RT is the notion of roles cluster head and cluster member. Each RT management principal has its own given name space for roles such as (Cluster Head, Cluster Membership), similar to localized name (highest trust values) spaces in trust management. For example, if K_A is a principal that is highest trust values and R is a role term of either Cluster Head (CH) or Cluster Membership (CM), then K_A . R is the role R defined by principal K_A with highest trust for each nodes and can be read as K_A R role. Only K_A can issue policy statements defining the role $K_A.R$. These statements determine members of $K_A.R$. For example, K_A can define $K_A.R$ to include another principal K_B role, effectively delegating some control over the role K_A R to K_B.

A cluster group is clearly a set of principles that has the highest trust values with less communication time for node to node communication. An identity is a set of principles corresponding to one physical user (Cluster Head (CH) to Cluster Member (CM)) some systems require the set to contain just one principle. To remove suspicious node in the network that are trustworthy (Crosby *et al*., 2006), Cluster head selection is important in WSN. A Role in RBTM can be viewed as a set of highest trust values that are members of this role. The role hierarchy relationship that $K_B.R$ is more powerful than $K_A.R$ can be viewed as defined that all members of $K_B.R$ are also members of $K_A.R$. Permission corresponds to a set of highest trust values given by the authorities. The highest trust amounts to each node in wireless sensor network set as a principal as each node of the set corresponding to the permission for each node in wireless sensor networks. Granting permission to a role (Cluster Head (CH) and Cluster Membership (CM) amounts to asserting that the cluster corresponding to the permission which a subset the set is corresponding to the roles Cluster Head (CH) and Cluster Member (CM). To understand our concept, first

define the role and principals for each roles in wireless sensor networks is based on the trust value that defines a rules to assign roles for each node, then formation of cluster. After that perform optimal path discovery for each clusters to eliminate malicious node.

Creating the roles for cluster head selection and cluster formation:

Sample calculation for role trust system: The role trust system consists of basic elements such as entities, role names, roles and policies. An entity represents number of nodes in the WSN that can characterize roles as Cluster Head (CH) and Cluster Member (CM). Role names represent permissions that can be concerned by one entity to other entities, or groups of entities. Highest trust value result considered as cluster head and the remaining nodes is considered as Cluster Member (CM). Roles represent sets of nodes that have particular permissions granted according to the access control policy for Cluster Head (CH) and Cluster Members (CM). Credentials define roles by selecting a new cluster member of the Cluster Head (CH) role by delegating authority to the members of other roles. Based on the Credentials, the Cluster Head (CH) and Cluster Members (CM) are selected and cluster creation is completed:

$$K_A.R \leftarrow K_B.S \quad (1)$$

Simple inclusion: Role $K_A.R$ consist of all members in the nodes role $K_B.S$.

This is a delegation of maximum trust values over r from K_A to K_B. Since K_B may reason new entities to become members of the role K_A r by issuing credentials that define $K_B.S$. Based on these roles, the Cluster Head (CH), Cluster Members (CM) are selected.

The cluster head role is created based on the lowest time communication level $K_A = \{higest\ trust\ value\ node\ with\ low\ Tv_{x,y}\}$ with N $K_B = \{nodes\ present\ in\ the\ system\}$ and $S = \{Trust\ values\ of\ each\ nodes\ Tv_{x,y}\}$ the afore mentioned policy compare the every time taken from previous interaction results where lesser communication time considered as higher trust value for cluster head selection. $K_B.S$ Compares every node of the time communication to K_A lower threshold then selected as Role Cluster Head (CH):

$$K_A.R \leftarrow K_D.R1 \leftarrow K_C.S \quad (2)$$

where,

K_C = Remaining nodes WSN
S = Trust values of remaining nodes $Tv_{x,y}$
K_D = Trust values of node except CH, cluster size
$R1$ = Cluster head members
R = Cluster head

If it satisfies $K_D.R1$ then cluster head members are added to cluster $K_A.R$. The time taken for communication are converted into descending order to formation of cluster, because if the present cluster head reaches dead state based on energy it automatically selects the second lowest time communication as cluster head. Three nodes are formed a cluster and added to K_A. Then remaining two nodes again perform the same policies (1) and (2). Next it performs the ABC algorithm is performing to select path in each cluster.

OPTIMAL PATH SELECTION USING ARTIFICIAL BEE COLONY (ABC) ALGORITHM

Earlier work (Karaboga and Akay, 2011) pertains to the development of optimized framework related to ABC and solves many real time optimization problems. The Algorithm replicates the intellectual searching behavior of honey bee swarm. In ABC algorithm, the gathering of artificial bees is considered as nodes where each node in cluster is divided into three types of bees: employee bees, onlookers and scouts. Each node in the cluster performs wait based on the dancing area for the best optimal path selection. Clustering is measured as optimal path and this bee is named as onlooker. The best optimal path appointment is considered as employed bee. The remaining bee in the WSN is named as scout bee that carries out random exploration for discovering new optimal path sources. This results in the assigning of optimal value in each cluster in a cluster role trust management system. The position of each node in a optimal path represents best optimal solution and the nectar amount is analyzed to calculate the quality (fitness) of the equivalent optimal path, it is calculated by using (3):

$$fit_i = \frac{1}{1+fit_i} \quad (3)$$

Each node sends a data to other nodes in the cluster, from which fitness values is estimated. In this study fitness function is evaluated based on weight function of a small number of parameters, like degree of the node in cluster, received power level for each node, trust factor and battery level. Trust values estimates the extension of earlier work (Bednarczyk and Gajewski, 2013). This parameter is calculated using the formula:

$$fit_i = D_G W_1 + P_R W_2 + T_F W_3 + B_L W_4$$

where, W_1, W_2, W_3, W_4 are weight values of the parameters like degree of the node in cluster, received power level for each node, Trust factor and battery level. The sum of the weight values should be equal to one. Change of weight parameter values can be continuously applied to several areas:

$$W_1 + W_2 + W_3 + W_4 = 1$$

Degree of the node (DG), as a number of edges of a given node, the Received Power level (PR), Trust Factor (TF), Battery Level (BL), as a remaining work time.

In the ABC algorithm, the nodes in the clusters are separated into two bee's employee and onlooker bee's. The first half of the nodes in the cluster are the employee bees and the second half of the nodes in cluster continues to be the onlooker's bee. The total number of employee bees in the cluster is equal to the best optimal path nodes in the cluster population. Initially the best optimal path is assigned to zero and each optimal path selection results in z_i where $i = 1, 2, \ldots, SN$ is a D-dimensional vector pertaining to the number of nodes in WSN. Corresponds to the cluster size for each group is initialized to the cluster population in WSN. The best optimal path of the location is selected and is focused to repeat based on the Maximum Number of iterations (MCN). An employed bee produces the best optimal path selection result and updates its memory based on current optimal path selection which results in the RTMS cluster. Corresponding updates in position of each employee bees is done (3). If they found optimal path selection results in cluster having better than the old selection optimal path than old cluster is replaced by the new one as best optimal path else the current optimal path as new one. All employed bees (nodes) in the cluster complete the optimal path selection. As they share the nearest nodes information with best optimal path selection. Onlooker bee evaluates optimal path selection resulting in the clustering of the employee bee. It then selects an optimal path with highest probability values related to new optimal path, Provided that the nectar node results in the path selection that has higher value than the earlier. The new employee bee nodes results in the best path selection in RTMS. Every node has a collection of probability values associated with that optimal path. Food sources for all neighbors' nodes and the cluster size will find out the probability of bees selecting a definite route or another definite route. Consequently, the food source is treated as the unit of trust. Yet, in order to differentiate between food source and trust value, T_i is defined as the trust value of node i, where $1 \leq i \leq k$. Trust value will be calculated based on food source from fitness function (3). An artificial onlooker bee chooses an optimal path selection depending on the fitness function (3). That corresponding positions are updated to each employee bee which results in the best optimal path selection with highest probability values p_i to each nodes, it is calculated by the following expression:

$$p_i = \frac{fit_i}{\sum_{n=1}^{SN} fit_n} \quad (4)$$

where, SN is the number of cluster size equal to the number of employed bees present in current cluster and fit_i is defined below:

$$fit_i = D_G W_1 + P_R W_2 + T_F W_3 + B_L W_4$$

In order to find best optimal path selection in the cluster with old memory path selection result, the ABC uses the following expression (5):

$$\mathrm{v_{ij}} = \mathrm{Z_{ij}} + \phi_{\mathrm{ij}}\left(\mathrm{z_{ij}} - \mathrm{z_{kj}}\right) \quad (5)$$

where, $\mathrm{k} \in \{1, 2, \ldots, \mathrm{SN}\}$ and $\mathrm{j} \in \{1, 2, \ldots, \mathrm{D}\}$ are randomly chosen indexes for optimal path selection in cluster. Although k is defined as random number it is varied from i. ϕ_{ij} is a random number between (-1, 1). This will result in reducing the production of neighboring path optimal sources around z_{ij} and represents the comparison of two optimal path positions visible to a bee. In Eq. (6), as the difference between the position of different nodes in cluster $z_{i,j}$ and $z_{k,j}$ decreases, the perturbation on the location $\mathrm{Z_{ij}}$ decreases, too. Thus, the search results to the optimal path selection in the search space, reducing the number of iteration. The optimal path selection of nectar bees is discarded by scout bees and it is replaced with new optimal path selection resulting in scouts clusters. In ABC, this is replicated by producing an optimal path selection location randomly and replacing it with the discarded path selection. In ABC, providing the best optimal path in cluster cannot be improved further during a predetermined number of cycles. The optimal path is assumed to be abandoned. Assuming that the discarded nodes paths is z_i^j and $j \in \{1, 2, \ldots, D\}$, then the scout bee discovers a new optimal path to be replaced with z_i^j. This operation can be defined as in (6):

$$z_i^j = z_{min}^j + rand(0,1)\left(z_{max}^j - z_{min}^j\right) \quad (6)$$

After each candidate optimal path selection it is estimated by artificial bee by pertaining to source position $\mathrm{v_{ij}}$ is formed. Its accuracy is compared with the old path selection. If the new path selection results in an equal or higher than earlier path selection results, then current path selection in cluster is selected as best path, else the present path is kept as the best path. In cluster and is determined to be the best path to send packet from source to the destination. On the other hand the selected old path is kept in the memory. In other words, a greedy path selection is employed as the best path selection among old and new path. There are three major control parameters in the ABC algorithm to be considered. They are the number of optimal food sources which is equal to the Single population (SN), the value of maximum value (MCN (Maximum Cyclic

Number)) to total number of the path selection. In a robust path selection process for each cluster, investigation and development processes are required to be carried out together in WSN. In the ABC algorithm, where both onlooker and employee bees carry out the investigation process in the path selection, the scouts bee control the development process of path selection in cluster. The local path selection results in ABC algorithm. The algorithm pertaining to the nearest node of cluster path investigation and greedy selection of each node is carried out and deployed in between the employed bee and onlooker. The entire path selection result in random search procedure performed by scouts'. Thereby the nearest path of the employed and onlooker bees is selected.

Proposed algorithm for optimal path selection using artificial bee colony:

Input: Cluster head and cluster member
Output: Best path discovery for cluster member to cluster head
Generate initial population; each cluster is considered as single population
$z_i, i = 1, \ldots, SN$
SN is the cluster size
Evaluate the fitness of each node in the cluster
Set $cycle = 1$
Repeat
For each employee bee
{
Produce a new optimal path with trust value v_i using
$v_{ij} = z_{ij} + \phi_{ij}(z_{ij} - z_{kj})$
Where z_{ij} is a path between the node i and j
Calculate the fitness value f_i for new path
Apply the greedy selection to select the best optimal path from the set of new paths
}
Calculate the probability value p_i for each optimal path selected from Eq. (4)
For each onlooker bee
{
Select a best optimal path z_i depending on probability p_i
Produce new path solution v_i
Calculate the fitness value f_i for new path
Apply the greedy selection to select the best optimal path from the set of new paths
If there is any abandoned solution for scout bee then replace it with new optimal path solution which will be randomly produced by (6)

Table 1: Simulation settings

Parameter name	Value
Number of nodes	600 to 1100 nodes
Initial energy/node	50 joules
Simulation time	1500 sec
Baseline node power	6 mW
Simulation runs	10
Packet size	300 bytes

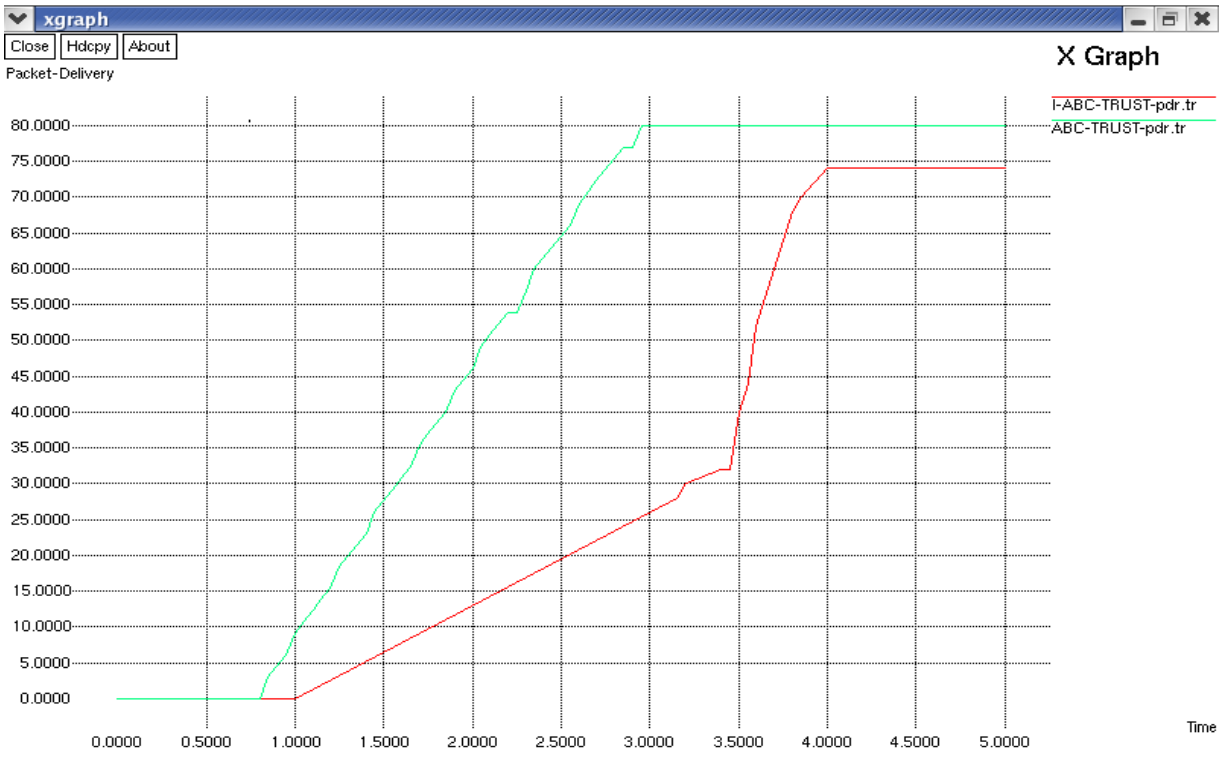

Fig. 2: Packet drop ratio vs. trust models

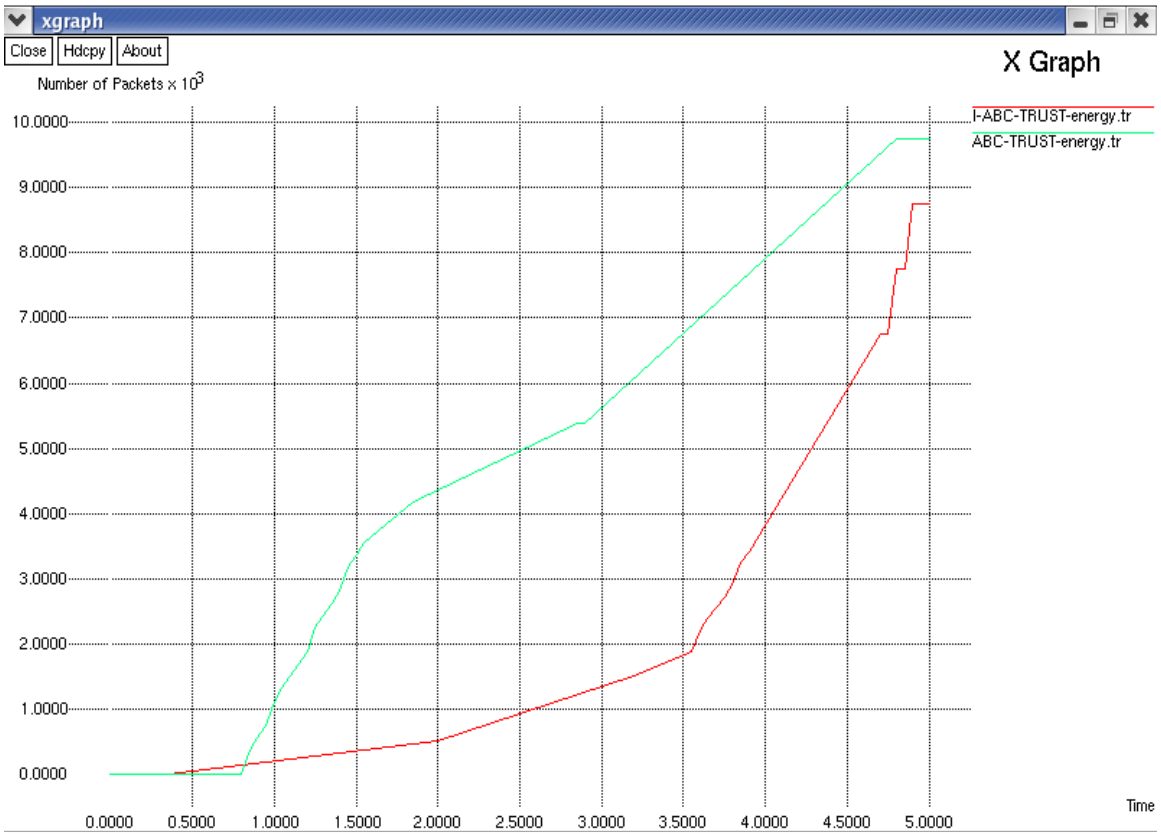

Fig. 3: Energy consumption vs. trust models

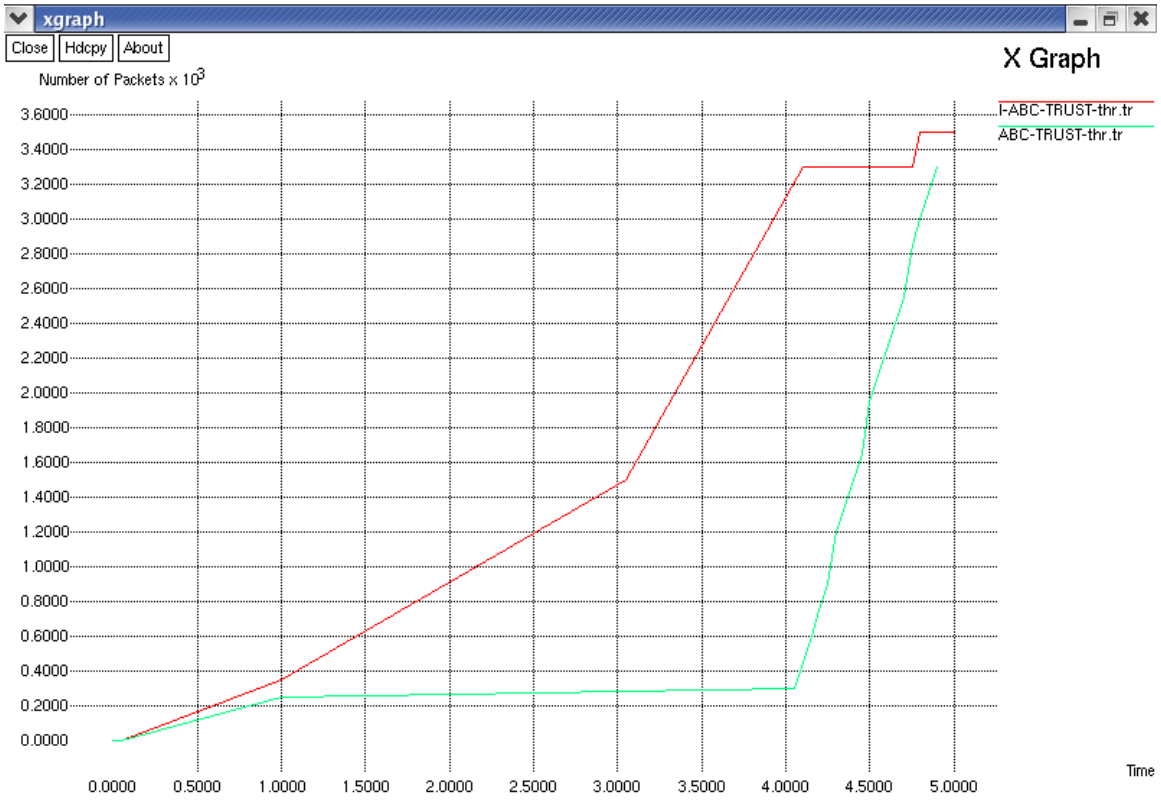

Fig. 4: Throughput vs. trust models

Memorize best optimal path so far
Cycle = Cycle+1
Until
Cycle = MCN

Cluster head is selected after the path selection. If the battery level of the ch is moves to the lower or dead state ABC path selection algorithm executed. Until all nodes are traced in WSN.

EXPERIMENTAL RESULTS

The performance of the proposed improved Role trust model from following aspects: First to decrease network packet loss rate, less energy consumption and higher throughput. In the proposed model, there is no difference between client's nodes and server nodes. During experimentation the trust management system with role, uses a horizontal and rectangular area of 800×400 m. On observation the proposed work reduces packet drop ratio and increase throughput. The Table 1 shows the simulation for experimental results.

In this graph Fig. 2 shows the packet drop ratio between trust management system among ABC and improved Role Trust management system, it shows that proposed system have less drop ratio than without Role trust in ABC.

Figure 3 shows the energy consumption between trust management system among ABC and improved Role Trust management system, it shows that proposed system have less energy consumption than without Role trust in ABC.

Figure 4 shows the throughput between trust management system among ABC and improved Role Trust management system, it shows that proposed system have more throughput than without Role trust in ABC.

CONCLUSION

In this study introduce the Role based Trust Management System (RTRMS) framework for wireless sensor networks. In this study role based trust management system elects cluster head based on roles and remaining nodes in cluster are named as cluster members. In this study we have proposed an Artificial Bee colony Role Trust Management system for WSNs, called ABCRTRMS-WSN. It has been seen Shown that bee colony food sources deposited by onlooker bees help next bees to find the most trustworthy server through the most reputable path all over the network. The resulted ABCRTRMS-WSN is more efficient and appropriate for universal WSN with less packet drop ratio and high throughput. In particular, the ABCRTRMS-WSN is very successful in decreasing energy consumption and packet drop ratio with higher throughput ratio than without role based ABC model. It shows that ABCRTRMS-WSN framework is sufficient and has high accurateness in avoiding malicious nodes from being a cluster head selected based on role trust framework.

REFERENCES

Aivaloglou, E., S. Gritzalis and C. Skianis, 2006. Trust establishment in ad hoc and sensor networks. In: Lopez, J. (Ed.), CRITIS 06. LNCS 4347, Springer-Verlag, Berlin, Heidelberg, pp: 179-194.

Bednarczyk, W. and P. Gajewski, 2013. An enhanced algorithm for MANET clustering based on weighted parameters. Univ., J. Commun. Network, 1(3): 88-94.

Chakaborty, A., S. Ganguly, M.K. Naskar and A. Karmakar, 2013. A trust based fuzzy algorithm for congestion control in wireless multimedia sensor networks (TFCC). Proceeding of 2nd International Conference on Informatics, Electronics and Vision (ICIEV, 2013). Dhaka, Bangladesh.

Crosby, G.V., N. Pissinou and J. Gadze, 2006. A framework for trust based cluster head election in wireless sensor networks. Proceeding of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS '06), pp: 13- 22.

Dhurandher, S.K., S. Misra, M.S. Obaidat and N. Gupta, 2009. An ant colony optimization approach for reputation and quality of-service-based security in wireless sensor networks. Secur. Commun. Network., 2(2): 215-224.

Ferraiolo, D.F., R.S. Sandhu, S. Gavrila, D.R. Kuhn and R. Chandramouli, 2001. Proposed NIST standard for role-based access control. ACM Trans. Inform. Syst. Se., 4(3): 224-274.

Ganeriwal, S. and M.B. Srivastava, 2004. Reputation-based framework for high integrity sensor networks. Proceeding of the 2nd ACM Workshop Security of Ad Hoc and Sensor Networks (SASN' 04), pp: 66-67.

Gorla, D., M. Hennessy and V. Sassone, 2006. Inferring dynamic credentials for role-based trust management. Proceeding of 8th ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP' 06). Venice, Italy, pp: 213-224.

Karaboga, D. and B. Akay, 2011. A modified Artificial Bee Colony (ABC) algorithm for constrained optimization problems. Appl. Soft Comput., 11: 3021-3031.

Lasota, K. and A. Kozakiewicz, 2012. Model of user access control to virtual machines based on RT-family trust management language with temporal validity constrains-practical application. J. Telecommun. Inform. Technol., 3: 13-21.

Li, N. and J.C. Mitchell, 2003. RT: A role-based trust-management framework. Proceeding of 3rd DARPA Information Survivability Conference and Exposition. Washington, DC, USA, pp: 201-212.

Li, F. and Y. Wang, 2007. Routing in vehicular ad hoc networks: A survey. IEEE Veh. Technol. Mag., 2(2): 12-22.

Li, N., W.H. Winsborough and J.C. Mitchell, 2003. Distributed credential chain discovery in trust management. J. Comput. Secur., 1: 35-86.

Marmol, F.G. and G.M. Perez, 2011. Providing trusting wireless sensor networks using a bio-inspired technique. Telecommun. Syst. J., 46(2): 163-180.

Ren, F.Y., H.N. Huang and C. Lin, 2003. Wireless sensor networks. J. Softw., 14(7): 1282-1291.

Shaikh, R.A., H. Jameel, B.J. d'Auriol, H. Lee and Y.J. Song, 2009. Group-based trust management scheme for clustered wireless sensor networks. IEEE T. Parall. Distr., 20: 1698-1712.

Yang, J., M. Xu, W. Zhao and B. Xu, 2010. A multipath routing protocol based on clustering and ant colony optimization for wireless sensor networks. Sensors, 10: 4521-4540.

Yao, Z., D. Kim and Y. Doh, 2006. Plus: Parameterized and local trust management scheme for sensor networks security. Proceeding of 3rd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS'06), pp: 437-446.

Zarei, M., A.M. Rahmani, A. Sasan and M. Teshnehlab, 2009. Fuzzy based trust estimation for congestion control in wireless sensor networks. Proceeding of International Conference on Intelligent Networking and Collaborative Systems.