Novel Approach for Reliable Communication in Wireless Sensor Networks Using DDRA

[1]Mr. V. KOVENDAN, [2]Mrs. S. SAROJINI

[1]Assistant Professor CSE, [2]Assistant Professor CSE,
Department of computer science and engineering,
Arasu Engineering College, Kumbakonam, TamilNadu, India

Abstract: **Energy protection is a significant issue in Wireless Sensor Node and also Authentication is the major problem in wireless sensor network. Subsequently energy management is a major problem in WSNs, data fusion and aggregation should be exploited in order to save energy. In this paper propose a novel Direct Diffusion Routing Algorithm (DDRA), this routing algorithm includes direct diffusion by means of PC and a clustering selection scheme, considering network topology and energy level of nodes. The goal is to create clusters which results in improve energy efficiency and decrease delay. It was determined DDRA construction that has the ability of refining delay and delivery rate in a fixed size scenario. The data Routing In-Network Aggregation is a system also generates two ways of authentication for reliable communication. It also indicates clearly that with the increase number of nodes, throughput & lifetime increases and simultaneously delay, energy consumption, and tree cost decreases. The proposed algorithm was conceived to improve the energy efficiency and also maximize information fusion. It provide Secure routing in ad hoc networks and provides Authentication, Access control, Confidentiality, Privacy, Integrity, Authorization, Anonymity, No repudiation, Freshness, Availability, and Resilience to attacks.**

***Keywords*: WSN, Reliable Communication, DDRA, Security, Routing**

I. INTRODUCTION

Security in the network is a greatest challenge in wireless communication, which can prevent and observer unauthorized person and network resources. Network security was controlled by the administrator to access the data in network. Users are assigned to some authenticating information that allows them access to programs within their authority. Network security covers a variety of computer networks, both public and private businesses leading transactions and transportations among businesses, governments and so on. Each and every Network should be private, such as within a organization, and others which might be open to public access. Network security it secures the network, as well as defensive and supervision operations being done while data or an info on a communication. The fine easiest way of shielding a network resource is by conveying it a unique name and the password. The sensor nodes, in-networking aggregation can often be used to reduction the communication rate by sending and reduce the duplication [2] with smaller aggregated information. Meanwhile it saves the energy to make nominal communication, which enlarges the network lifetime; in-network data aggregation is a key method to support the WSNs.

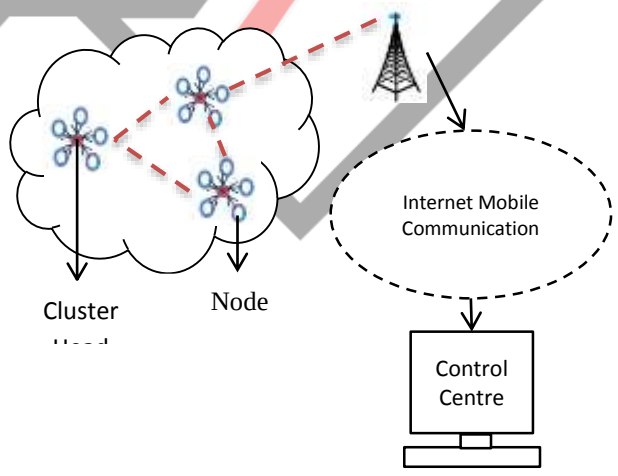

Fig. 1 wireless Sensor Network Architecture

In this context, the use of information fusion is double: (i) to take advantage of data redundancy and increase data accuracy, and (ii) to reduce communication load and save energy.

2. PROBLEM DEFINITION

Reliable communication in Wireless Sensor Networks is the context of WSN; data aggregation [10] aware routing protocols should present some desirable characteristics such as: a reduced number of messages for site up a routing tree and increases of

overlapping routes, high aggregation rate. So we propose a new techniques novel Direct Diffusion Routing Algorithm for WSNs, which we refer to as DDRA algorithm [4] was conceived to maximize information fusion along the communication route in trustworthy way, through a fault-tolerant System.

The existing cluster based approaches are tree based approaches, cluster based schemes also consists of a hierarchical organization of the network. In Information fusion based role assignment (InFRA) algorithm, when multiple nodes detect the same event, they organize themselves into clusters. Then the cluster-heads aggregate data from all cluster members and send event data towards the sink. Since all nodes may not directly reach the sink node, the notification packets are relayed in a multi-hop fashion. The existing procedure increases the communication cost of the algorithm.

- The existing systems provide limited scalability.
- Low performance and high computational cost.

3. PROPOSED SYSTEM AND IMPLEMENTATION

To develop an accurate algorithm for a Direct Diffusion Routing Algorithm (DDRA), that has some key aspects such as a reduced number of messages for setting up a routing structure tree, max number of overlapping. This system also generates two ways of authentication for reliable communication. It also indicates clearly that with the increase number of nodes, throughput & lifetime increases and simultaneously delay, energy consumption, and tree cost decreases. Which can results reliable communication on the wireless sensor network by clear routing methodology and secured path identification with the help of key generation from the server based on th request message. And the DDRA algorithm [4] has the following advantages on various routing schemas as given below

3.1 Advantages of Routing Schemes of Algorithm

a. Routing Schemes – Any cast
Data is routed to the "nearest" or "best" destination; Destinations identify a set of host only one is chosen
b. Routing Schemes Broadcast
Data is routed to everyone, Used with Discovery Protocols, Can only be sent to nodes on that network segment
c. Routing Schemes Multicast
The group delivery of data to everyone, receiver node can find a set of host and data is delivered to the whole set, used with IRC, Video streaming
d. Routing Schemes Unicast
Data is sent to one destination, Used with Http, SMTP, POP, SSH, most services, Compared to traditional methods, Routes are established on command, No attempts to find a pre-defined free-loop path and as message caches are used for loop avoidance.
The proposed system was conceived to max information merging along the communication route in dependable way, over a fault-tolerant routing mechanism. DDRA provide Secure routing in ad hoc networks and provides Authentication, Access control, Confidentiality, Privacy, Integrity, Authorization, Anonymity, No repudiation, Freshness, Availability, and Resilience to attacks. The proposed system reduces the number of messages for setting up a routing tree. The proposed systems provide two ways of authentication for reliable communication. Increase lifetime. The proposed system provides Authentication, Access control, Confidentiality, Privacy and Integrity.

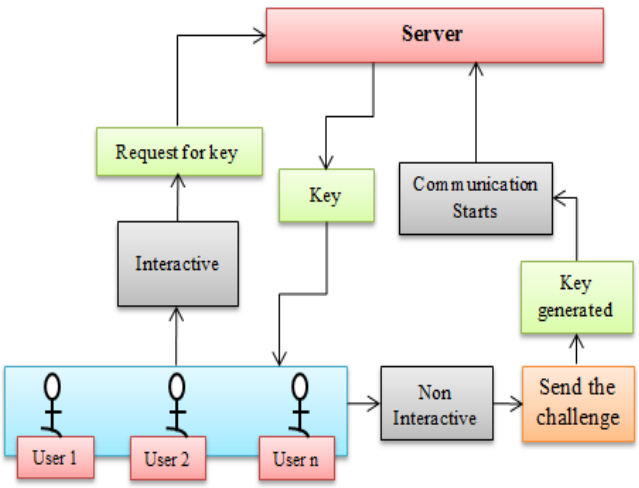

Fig.2. System Architecture

3.1 Challenge Your Neighbor

To challenging your neighbor is, to add a new node in a network. A node having its neighbors in its friend list does not need to challenge them before a data session. When a new node is initialized in a network, each node is become as a stranger to each other another for the resources. So thus each node integrates with its neighbors no within the unauthorized list. The node picks one of the neighbors, and performs the usual Share Friends Stage. As a response the neighbor node either sends its friend list or the nodes from its unauthenticated list if the friend list is empty.

3.2 Rate and Share Friends

Initially each node has completed the challenge successfully with their friend list and the sharing of friend nodes is done in the share stage as the friend relation is transitive in nature that is if a friend of is and is a friend of includes in his friend list too. Friend sharing is a periodic process which is chiefly responsible for the security of the algorithm. FREQ (Friend request for sharing is used to accomplish friend sharing to control packet) and the node replies for the request with the nodes in its friend list, unauthenticated list and the question mark list.

3.3 Routing Efficiently

Through the single routing path the data sending and receiving can be done within the time, that should be increased and the data rate can be decreased. The data sharing performance can be delayed by the present using algorithms. The data can be send and receive through set the path using the genetic algorithm to efficiently send the data to the receiver and the data rate can be greater than before and it can set the alternate path to transfer the data and it leads to increase the data rate and net rate to an efficient scheduling of data to be shared efficiently**.**

4. TEST AND RESULT

Login phase

In the login form the username and password are displayed. Here the error occurred is the password characters are displayed transparently. The password characters whatever entered by the user should not displayed in text characters. The password should be hide using some special characters like (*, #, $). By using the special characters the password will not easily hacked by the other users.

The test cases for our system are as given below with the following screen shots.

Test Case 1: Server

The server can able to start and stop the server. The user can able to connect with the connected client list. The inactive user list can be viewed by the Server. The message box displayed as Start server.

Test Case 2: Select User

The new user can able to register their details Selecting New User. The user who already registers can use the Existing User.

Test Case 3: Interactive User

The user can able to select the interactive and non-interactive and to enter the user name and the key will be generated in the SQL server. The users copy the key and paste the key in the interactive form. The message box will be displayed as user joined in network. In this project there are server create two users in interactive section.

Test Case 4: Client

The user can able to generate key for the user who select the non-interactive. The RSS and RTT will generate automatically to the client.

Fig. 4.1 Interactive User - joined to the network

Non Interactive User

The non-interactive user is created to communicate with the client and to send the challenge to the user. The username will be displayed in the connected list. The message box displayed as challenge sent. The other message box will be displayed as assistant sent to user whatever the user select

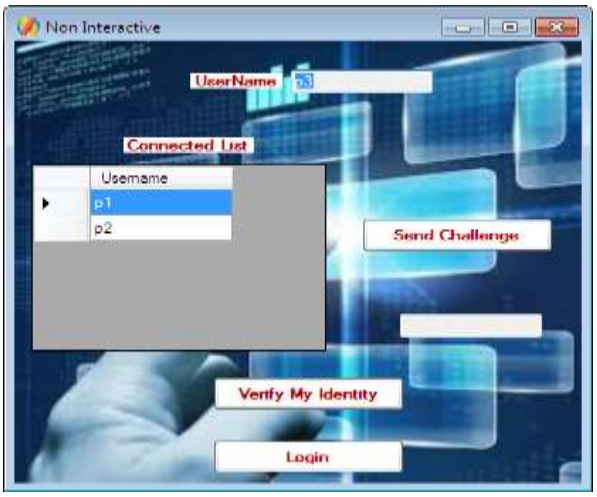

Fig. 4.2 Non Interactive User

Test Case 5: Generate and Verify key
The user can able to verify the key. Here the user who sends the challenge using the non-interactive can able to receive the key from the friend user can view the key which is automatically generated.

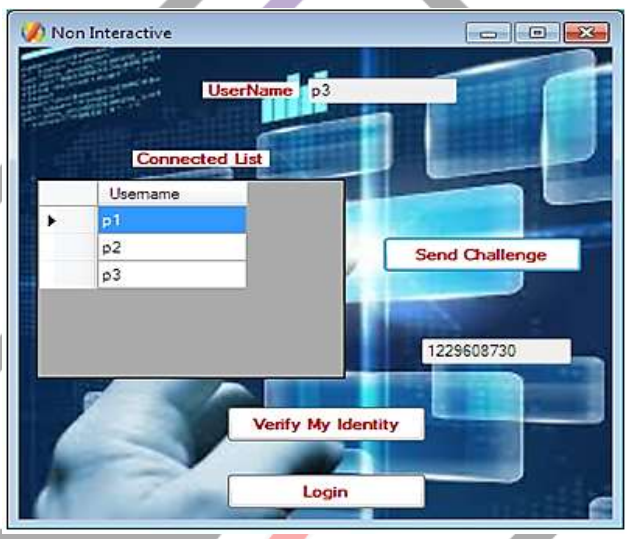

Fig.4.3 Generate and Verify key

Test Case 7: User Login Using Non Interactive User
The user can able to view the connected list and the user can able to select the data. The message box displayed as Data transfer in new path and Path will also displayed.

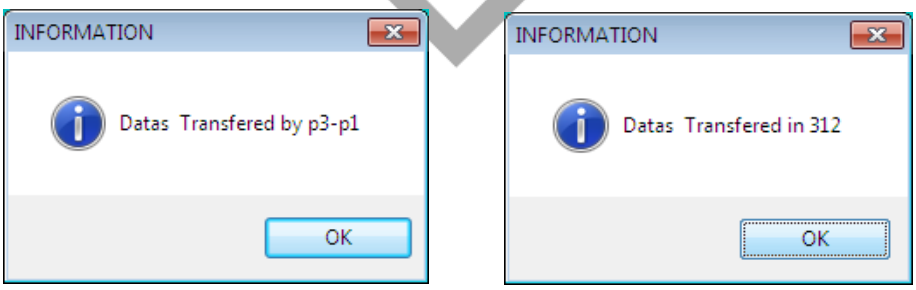

Fig 4.4 Verifying the key

6. CONCLUSION

The system generates two ways of authentication for reliable communication. It also indicates clearly that with the increase number of nodes, throughput & lifetime increases and simultaneously delay, energy consumption, and tree cost decreases. Thus the routing algorithm would conceive to maximize information fusion along the communication route in reliable way, through a fault-tolerant routing mechanism. Direct Diffusion Routing Algorithm provide Secure routing in ad hoc networks and provided a Authentication, Access control, Confidentiality, Privacy, Integrity, Authorization, Anonymity, No repudiation, Freshness, Availability, and

Resilience to attacks, and also provides the energy concussion. In a future work, direction is to study and improve the performance of this construction method and eventually develop new and better distributed/localized solutions.

REFERENCES

[1] F. and Heidemann, J. Stann, "RMST: Reliable Data Transport in Sensor networks," in Proceedings of the First IEEE International Workshop onSensor Network Protocols and Applications , 2003, pp. 102- 112.

[2] K., Neelisetti, R. and Lim, A. Casey, "RTDD: A Real-Time Communication Protocol for directed diffusion," in IEEE Wireless Communications and Networking Conference (WCNC,08), 2008, pp. 2852-2857.

[3] Ning Hu and Deyun Zhang, 2006. Source Routing Directed Diffusion in Wireless Sensor Networks. Information Technology Journal, 5: 534-539. DOI: 10.3923/itj.2006.534.539

[4] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estfin, John Heidemann, Member, IEEE, and Fabio Silva, "Directed Diffusion for Wireless Sensor Networking" IEEE /ACM TRANSACTIONS ON NETWORKING, VOL. l 1, NO. 1, FEBRUARY 2003

[5] Mohammad Abdus Salam and Tanjima Ferdous"CHARACTERIZATION OF DIRECTED DIFFUSION PROTOCOL IN WIRELESS SENSOR NETWORK"Southern University, Baton Rouge, LA 70813, USA International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 3, June 2014

[6] G. Anastasi, M. Conti, M. Francesco, and A. Passarella, "Energy Conservation in Wireless Sensor Networks: A Survey," Ad Hoc Networks, vol. 7, no. 3, pp. 537-568, http://dx.doi.org/10.1016/ j.adhoc.2008.06.003, May 2009.

[7] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cyirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, Mar. 2002

[8] K. Romer and F. Mattern, "The Design Space of Wireless Sensor Networks," IEEE Wireless Comm., vol. 11, no. 6, pp. 54-61, Dec. 2004.

[9] C. Efthymiou, S. Nikoletseas, and J. Rolim, "Energy Balanced Data Propagation in Wireless Sensor Networks," Wireless Networks, vol. 12, no. 6, pp. 691-707, 2006.

[10] B. Krishnamachari, D. Estrin, and S.B. Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks," Proc. 22nd Int'l Conf. Distributed Computing Systems (ICDCSW '02), pp. 575-578, 2002.