Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.264 – 270

RESEARCH ARTICLE

An Authentication Inclusive Preventive Model to Optimize Communication in WPAN

Sandeep Kumar
Student, M.Tech, Prannath Parnami Institute of Mgt. & Technology, Hisar, Haryana
sandeepbeniwal045@gmail.com

Gagandeep
Asstt. Professor, CSE Dept, Prannath Parnami Institute of Mgt. & Technology, Hisar, Haryana
Gagandeep.b.ppimt@ppu.edu.in

Abstract: As of the any public access network, WPAN also suffers from some internal or external attacks. To provide the reliable communication there is requirement of some preventive routing model. In this present work, an authentication improved preventive model is presented for secure and reliable communication. At first level of this model, the node authenticity is verified using RSA approach and later on HMM approach is provided to perform the association analysis among neighboring nodes. The communication parameters are analyzed using HMM approach to identify the safe and effective neighbor. This neighbor is elected as next communicating hop. By electing the effective next hops on each stage, the preventive route is generated. The implementation of work is implied in NS2 environment. The comparative result shows that the presented work model has improved the communication throughput and reduced the loss.

Keywords: WPAN, Preventive, Authentication, HMM, RSA.

I. INTRODUCTION

WPAN (Wireless Personal Area Network) is having its significance in limited area network. This network model is defined under mobility vector along with centralized controller. This controller nodes communication control so that the network effectiveness and the preventive mechanism from the outer environment can be achieved for the network. As the network also allow the public and global access to the network nodes, the network suffers from different kind of attack. The dynamic mobility and topology increases the security challenges for the network. The network requires some safe and secure mechanism for reliable communication so that the communication criticality will be reduced. The basic characteristics of network include cooperative network communication and resource adaptive communication in dynamic network. To provide the significant communication with limited resources is required to manage under protocol specification. Zigbee is one such protocol applied to enhance the network performance and reliabilty. Zigbee provides the communication evaluation for improving the communication reliability. The dynamic network models applied under zigbee network are shown in figure 1.

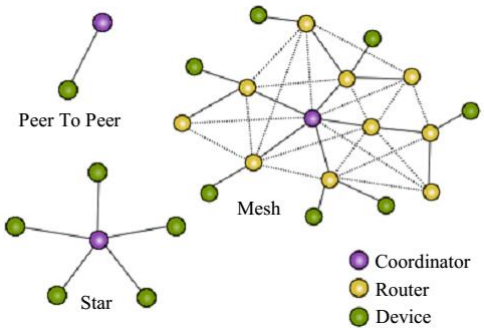

Figure 1 : Zigbee Network Models

These network model support the routing protocol specification under the zigbee standard specification. This protocol is able to maintain the communication route and path formation so that the robust route formation will be done. The route formation can be applied here by generating the request to the neighbor nodes. The route request (RREQ) is performed in this network for packet forwarding to neighbor nodes. The RREQ packet contains the source and destination information along with hop count and broadcast id with each associated node. The communication adaptive reverse path formation can be achieved using RREQ forwarding. This intermediate node identification process can be applied till the complete route is not formed. As the attack occur over the network, the route lost or the route error can occur over the network so that the broken link formation can be obtained over the network. The basic communication process applied by the zigbee protocol for route formation is shown in figure 2.

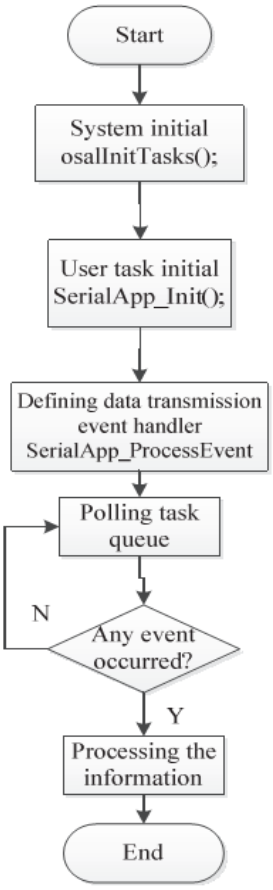

Figure 2 : Communication Process in Zigbee.

This zigbee based communication model is divided in three main stages. In first stage, the initialization of the task is done which is followed by the task queue polling to identify the effective resource. Finally the communication process is performed to achieve the transparent communication in the network.

In this work, a authentication and preventive model for route formation in zigbee network is defined. In this model, the RSA integrated HMM approach is defined for route generation. In this section, the security challenge in WPAN network is defined. The section also includes the route formation in zigbee network. In section II, the work defined by the earlier researchers is defined In section III, proposed work model is described. In section IV, the results obtained from the work are presented and discussed. In section V, the conclusion obtained from the work is presented.

II. EXISTING WORK

Different researchers already providing secure and safe routing model along with different algorithmic approaches and parameters formulation. Some of the work defined by earlier researchers is discussed in this section. Chen Peishan[1] has provided a work on zigbee based energy algorithm to generate the using path under cluster head analysis. Author generated cluster tree under AODV algorithm approach so that the route level assessment and route formation will be done. Author provided the communication analysis under residual energy analysis, energy balancing and data transmission so that the communication life time will be optimized. Author[2] has provided a secure routing approach for sensor network. Author provided the work on complex scenario analysis under the critical tissue analysis. This model includes the thermal aware communication route formation. Author obtained the route traversing model and provided the energy constraint formation so that the communication optimization will be achieved. Jinbao Li[3] provided a work on multiple parameter based communication control method so that the opportunistic route will be formed. Author provided the concurrent communication and packet scheduling so that the communication under critical scenario will be formed. Author provided the complexity adaptive route formation model in real time communication network to achieve the route formation in polynomial time. This communication is formed under efficiency and transmission delay constraints. Shuguang Xiong[4] provided a work on structured communication so that the network deployment will be achieved. Author provided the location derived communication so that the structured and constraint specific communication will be formed. The coverage range analysis is required for network deployment for optimized and constraint adaptive path formation.

M. M. Chandane[5] provided a work on quality aware communication in sensor network and provided the route formation under fading constraint. Author provided the multipath route formation so that the communication optimization will be achieved. Author[6] provided a work on geographical optimized scheduling routing model under constraint specification. Author provided the forwarding route formation and route optimization with two phase method. The communication optimization is achieved over the network under multiple constraints. Ming-Shing Kuo[7] presented a work on opportunistic routing model applied as a framework to the communication network. Author reduced the energy consumption over network and provided the optimized network communication. Author provided the reduction in energy loss and generates the adaptive communication routes. Amir Hossein[8] provided a work on energy effective route formation and communication quantization analysis. Author provided the route formation and effective routing model with relative parameters so that the network criticality will be reduced. Ting Lu[9] has provided an energy consumption reduction model by generating the multipath routing for communication network. Author provided the delay analysis model to generate the effective route with error rate reduction and reducing the energy rate. Deng[10] provided the routing model against the black hole attack. Author provided the node pair identification so that the malicious node identification will be formed. Author provided the route reply analysis so that the communication hop identification will be done. The matric based analysis model is defined for node confirmation model is defined for route optimization. The network route reformation is provided by the author.

III. PROPOSED MODEL

WPAN is the critical private area network which provide the public access because of which the network suffers from internal and external attacks. To provide the secure and reliable communication over the network, there is the requirement of some intelligent and predictive communication approach. The presented work has provided the solution against the public and the private network. To save the network from external public nodes, the authentication scheme is applied and to provide the secure communication route over the network, the HMM integrated routing model is

presented in this work. The presented work is divided in three main stages. In first stage, the communication network is established under the constraints specification. In this stage, the network constraints and restrictions are defined. As the network is formed, the second stage is defined to analyze the node under authenticity vector. In this stage, RSA based cryptography algorithmic is applied to perform the safe communication. As the nodes are verified, the communication analysis is performed on the neighboring nodes using HMM based predictive approach. This approach is defined to identify the safe and reliable nodes in terms of communication delay analysis and communication loss analysis. The process is repeated till the complete network path is not formed. The presented work model is shown in figure 3.

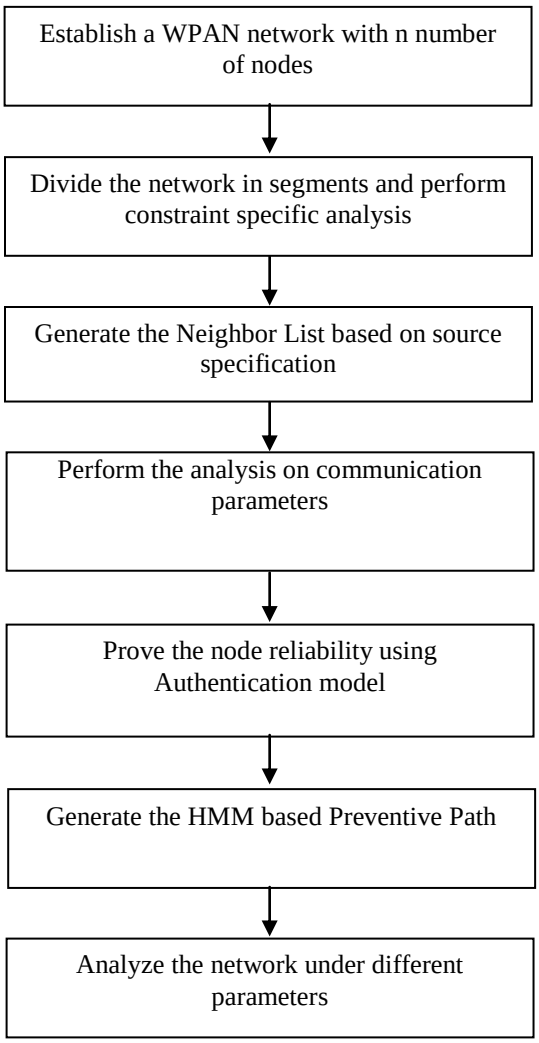

Figure 3 : Proposed Work Model

Here figure 3 is showing the proposed work model. The work flow shows that the work has at first constructed the network with node specification. Later on the communication analysis is performed by dividing the network in smaller segments. While performing the communication at first the node level authentication is verification is done using RSA approach. Now the list of neighboring nodes is obtained on the authentication adaptive reliability. The communication analysis is applied on these neighbor nodes to identify the node with minimum communication loss and delay. The HMM model is applied to generate the communication path. The work is defined to provide the reliable communication over the network. The implementation of work is done in maltab environment so that the safe communication path will be formed over the network.

IV. RESULTS

The presented work model is implemented in NS2 environment with formation of a random network. The network parameters related to this work are defined in table 1.

Table 1 : Communication Parameters

Parameter	Values
Area	50x50
Number of Nodes	25
Connection Agent	UDP
Traffic Type	FTP
Routing Protocol	AODV
Simulation Time	50 sec
Packet Size	512 Byes
MAC Protocol	802.15.4
Source Node	1
Destination Node	10

These parameters include the architectural parameters as well as communication parameters. The comparative analysis of this work is done in terms of communication throughput and communication loss. The figure 4 is showing the comparative analysis of this work with existing communication model in terms of packet communication over the network.

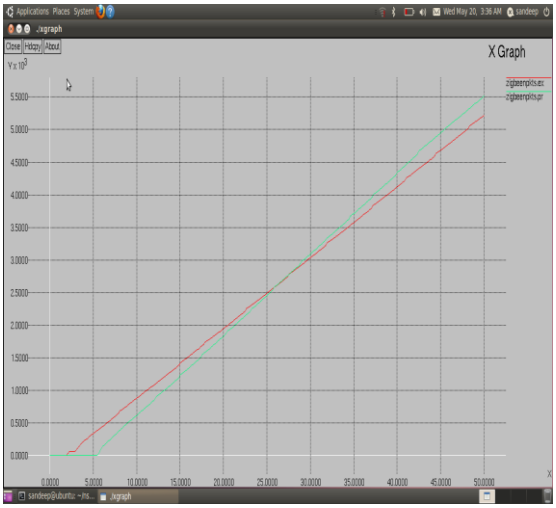

Figure 4 : Communicaiton Throughput
(Existing Vs. Proposed)

Here figure 4 is showing the comparative analysis of existing and proposed work in terms of communication throughput. The results shows that the presnted work has improved the communicaiton throughput in effective time.

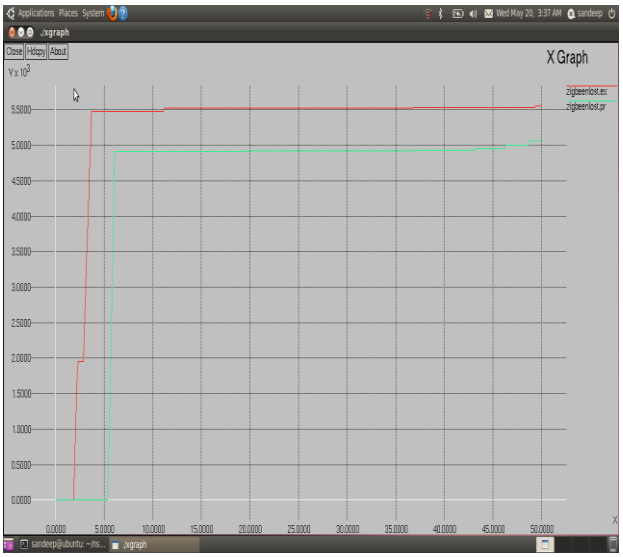

Figure 5 : Commpucation Loss
(Existing Vs. Proposed)

Here figure 5 is showing the communication loss anlaysi for existing and proposed approach. The figure shows that the presented work has decreased the communication loss over the network.

V. CONCLUSION

In this presented a robust and dynamic model is presented to provide the safe and secure communication over the network. This proposed model is divided in two phases. In first phase, authentication is provided using RSA approach to perform communication on reliable internal nodes. In second phase, the HMM based predictive analysis is provided to generate the safe communication path.

REFERENCES

[1] Chen Peishan, "Zigbee Energy Algorithm Based on Fusing Path Optimization and Cluster Heads Rotation", 978-1-4799-2860-6/13 ©2013 IEEE

[2] Chunsheng Zhu, "Sleep Scheduling Towards Geographic Routing in Duty-Cycled Sensor Networks", International Conference on Distributed Computing and Workshops, pp 1-3, 2011.

[3] Jinbao Li, "Joint Routing, Scheduling and channel assignment in Multi-Power Multi-Radio Wireless Sensor Networks", International Conference on Performance Computing and Communication, pp 1-8, 2011.

[4] Shuguang Xiong, "Efficient Algorithms for Sensor Deployment and Routing in Sensor Networks for Network-structured Environment Monitoring", Proceedings IEEE INFOCOM, pp 243-248, 2012.

[5] M. M. Chandane, "Distributed Link Quality Aware Routing in Wireless Sensor Network", International Conference on Computer Science and Automation Engineering, pp 528-532, 2012.

[6] Chunsheng Zhu, "A Geographic Routing Oriented Sleep Scheduling Algorithm in Duty-Cycled Sensor Networks", IEEE ICC 2012 - Wireless Networks Symposium, pp 5473-5477, 2012.

[7] Ming-Shing Kuo, "Joint Design of Asynchronous Sleep-wake Scheduling and Opportunistic Routing in Wireless Sensor Networks", IEEE Transactions on Computers, pp 1840-1846, 2012.

[8] Amir Hossein Mohajerzadeh, "Optimum Routing and Scheduling for Estimation in Wireless Sensor Networks", International Conference on Computer and Knowledge Engineering (ICCKE) , pp 243-247, 2012.

[9] Ting Lu and Jie Zhu, "Genetic Algorithm for Energy-Efficient QoS Multicast Routing", IEEE COMMUNICATIONS LETTERS, VOL. 17, NO. 1, JANUARY 2013

[10] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks, "communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

