International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A Parameteric Decision Rule based Neighbor Discovery Method for Effective Communication in WPAN

Sonia Sharma[1], Radhika Garg[2]

[1]*Student, M.Tech. (CSE), Vaish College of Engineering, MDU (India)*

[2]*Asstt. Prof., CSE Dept., Vaish College of Engineering, MDU, Rohtak (India)*

ABSTRACT

WPAN is the personalized network that provides the data and voice driven communication in the limited personalized area. The mobility and the energy specification increase the network criticality. In this work, a multiple parameter based neighbor discovery method is applied to generate the effective Communication in the WPAN network. The network is defined with specification of infrastructure devices. The communication is route is formed from each mobile sensor node to the infrastructure device. At the initial level energy and coverage based analysis is performed for neighbor identification. Later on, the effective node based on the connectivity and load is identified. The proposed model is implemented in NS3 environment. The proposed model is implemented on different network areas and with different node mobility. The results show that the proposed approach has improved the communication in mobile network.

Keywords: WPAN, Sensor Network, Cooperative Communication, Mobile Nodes

I. INTRODUCTION

WPAN is the challenging network form in which the specialized mobile devices are defined in the personalized area. The specialized mobile devices are defined with energy, memory and processing capabilities. The network is composed with specific scenario and topological constraint. The dynamic communication in this network is controlled using controller devices and the inclusion of GPS technology to each mobile sensor device. The GPS device is able to track the current position and the movement of the node. The specialized GPS based infrastructure devices are defined to track the devices and to improve the network communication. The GPS enabled network is shown in figure 1.

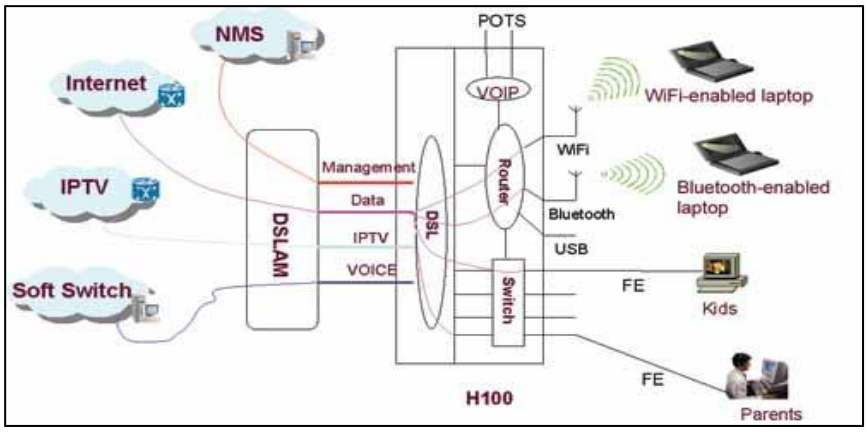

Figure 1: GPS Enabled WPAN Network

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Fig. 1 is showing the personalized area network defined for a home network. The figure shows that all the smart devices of kids, parents and other family members are connected through WiFi or Bluetooth network. The laptops, mobile phones can communicate to the global world in this network. The connectivity of this network is also provided to the IPTV, Soft Switch network and the internet. The data and voice communication is possible in this network form.

GPRS system can be established to any mobile network by performing the packet level node tracking in the network. The significant communication based on the data channel and the node level verification. The node connectivity and channel analysis can be achieved for the packet switched network. The circuit switched network can be composed for effective packet delivery in the exclusive network form. The packet switching based call setup and the delay reduction is also provided by this network form. The immediate access to the network is provided for the digital network form. The signal support is provided on different frequencies for different countries and the regions. GPRS is also responsible to improve the network communication and voice communication. The communication quality can be improved in a packet switched network by establishing the network form. The packet level communication establishment and the seamless tracking in hybrid network form is also achieved by using GPRS. The critical handoff mechanism, cluster switching and the base station transition is also achieved by this network form. The data transition in this advanced network form is provided to improve the communication reliability.

In this paper, a load and connectivity preserved communication in the personalized area network is provided. In this section, the introduction to the WPAN network is provided along with architectural characterization. The WPAN devices are equipped with GPS technology and based on this the node level tracking can be done. The position and movement analysis to the network is defined in this section. In section II, the work provided by the earlier researchers is discussed. In section III, the proposed research methodology is provided. In section IV, the results obtained from this work are provided. In section V, the conclusion of work is presented.

II. RELATED WORK

Lot of work is provided by the researchers to improve the communication in wireless personal area network. In this section, the contribution of researchers is discussed. Author[1] has defined the security adaptive communication method for personalized area network. The node coordination analysis with relevancy observation is provided. The system level, operational level communication and security behavior is discussed in this paper. Author[2] has defined a trust enabled communication in the personalized area network. The computational cost based analysis was provided in this work to optimize the network communication. The group adaptive trust mechanism is generated to optimize the network communication. The key adaptive relationship and the security model are provided to achieve secure and reliable communication in the network. Author[3] has defined feature adaptive network model to explore the various security constraints in this network. The descriptive observation to the different networks and the implementation based on the different scenarios is also provided in this paper. Author[4] has defined the work on jamming attack detection and to define a preventive routing in the critical network. The preventive route formation is provided to achieve the safe and reliable communication. The defensive communication model is provided to achieve the neighbor specific communication. Author[5] has used the ACO based defensive model to provide the effective communication in

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

personalized area network. The distributed network model is defined under different communication constraints. The opponent specific observation is defined to identify the certainty factor in the network. The traffic condition based observation is provided to improve the network communication. The traffic condition driven optimized communication is provided in this work.

Author[6] has defined the GPS enabled node tracking to identify the network attack and to provide the communication in case of security flaws. The time stamp based communication is provided to achieve the featured communication. The pre-observation to the network is provided against different attacks and to generate the safe network communication. Author[7] has provided a group based trust evaluation in the topological WPAN network. The inter-group analysis with relevant communication features is provided to achieve the security integration and to provide the symmetric communication. The segmentation specific cryptography method is provided to achieve the secure and reliable communication in the network. Author[8] has defined an analytical model to achieve the featured characterization to the topological structure of a personal area network. The safe communication based on the node position analysis is defined to provide the directional observation. The attack preserved communication is provided and to generate the selective routing in the network. Author[9] has defined a cooperative message communication and verification so that the constraint validation based communication will be performed. The probabilistic analysis is provided to analyze the security flaw and to generate the reliable communication in the network. Author[10] has defined the position adaptive analysis to provide the reliable communication in the WPAN network. The architectural improvement to the network is provided based on the distance and position driven node tracking. The communication and positional integration is provided in this work.

Author[11] has defined the statistical observation based structure analysis to generate the network signature and to perform the communication. The mobility driven analysis is defined to perform the regular monitoring of network node so that the improvement to the reception rate will be obtained. The communication latency reduction method is also suggested by the author. Author[12] has defined the content level symmetric feature observation is defined to improve the network communication and to reduce the communication loss. The black box observation is provided under the probabilistic measure to improve the network communication. The node level reputation is provided to generate the safe communication route in the constraint specific network. Author[13] has defined the communication framework to analyze the communication and the security constraints. The secure and trust adaptive communication is provided. The group specific network observation is defined to improve the communication capabilities.

III. RESEARCH METHODOLOGY

WPAN is the smarter mobile network defined for restricted and personalized geographical area. The nodes in WPAN are mobility nodes with energy restriction. Each node is having the larger memory space to manage the routing information. In this paper, an optimized neighbor discovery method is provided for WPAN network. Each of the router nodes will observe the current node and the next node under energy, load and communication constraint parameters. The selection of the next node will be done based on interaction analysis. The multiple decision criteria on intermediate selection will be done based on load, connectivity and energy parameters. The decision rule will be applied on each intermediate node of the communication route. The control message will

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

be defined for adaptive selection of neighbor nodes. The route discovery method is presented under energy, load and connectivity analysis. The dynamic route formation and optimized neighbor generation is defined by setting up the rules on these parameters. The flow of work is shown below in figure 2

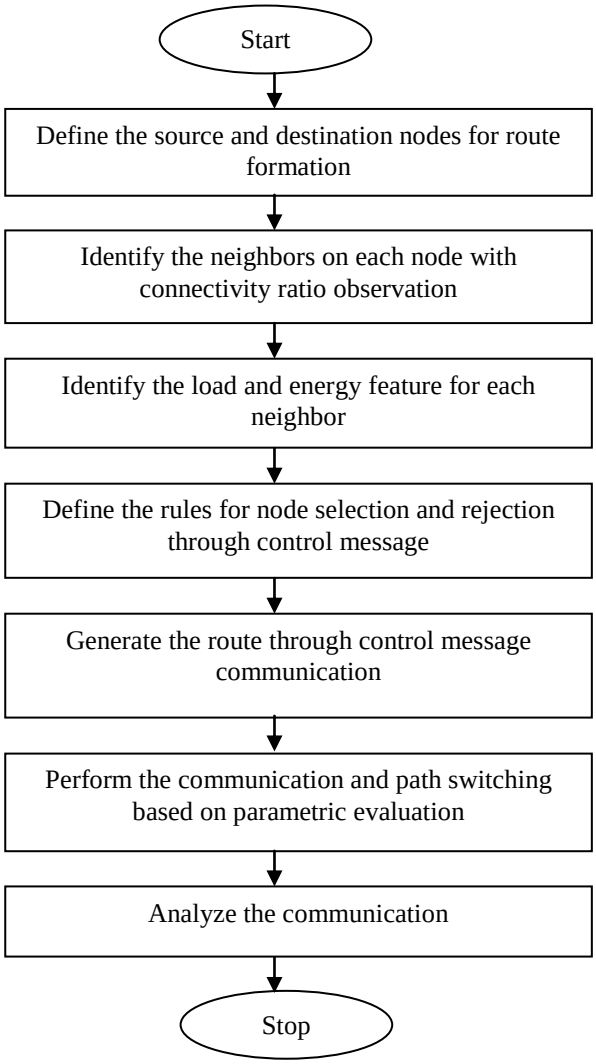

Figure 2 : Flow of Work

Figure 2 has shows the flow of work of this work to provide the safe and reliable communication over the network. The network is performed to generate the connectivity ratio analysis and to provide the control message communication so that the node selection will be done based on the effective node evaluation. The figure showing the parametric analysis on the node evaluation and to provide the control specific communication flow observation. The load and energy features are analyzed for each node for effective route formation in the network. The simulation results of this algorithmic model are shown in next chapter.

IV. RESULTS

The work model defined in previous section is about to optimize the communication in WPAN network. The neighbor node evaluation is provided based on the energy, load and coverage parameters. The connectivity observation is provided to identify the effective neighbor and to generate the reliable communication path

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

between each node of network and the infrastructure controller. The proposed work model is implemented in NS3 environment. The network is defined on a fix geographical area with 20 nodes. The network is defined with specification of fixed base station and the WiFi controller. The network is implemented with 5 different scenarios. The scenarios are defined based on the different mobile speed from lower to higher. The results are obtained in terms of packet drop rate and the communication rate. The simulation results are provided in this section

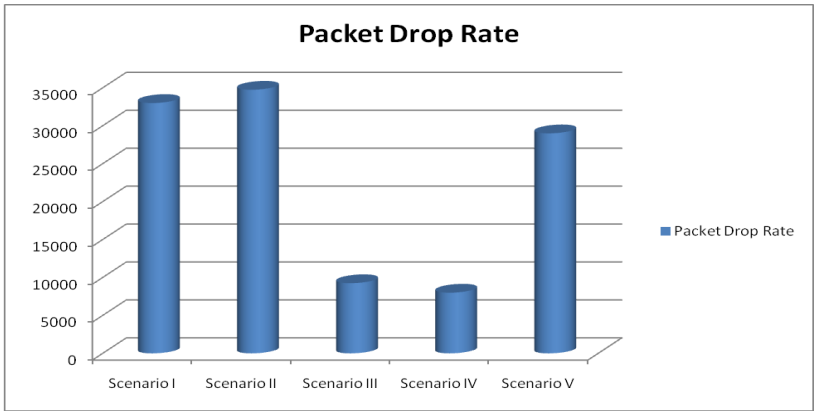

Figure 3: Drop Rate Analysis

Here figure 3 is showing the analysis of the proposed WPAN network communication under the mobility variation. The horizontal labels are showing the scenario names. The packet drop rate is shown in the figure. The figure shows that as the mobility is increased in the network, the communication lossrate is increased.

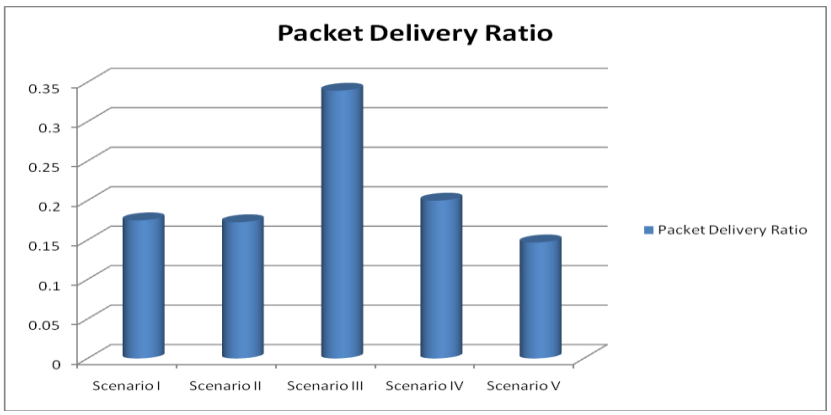

Figure 4: Packet Delivery

Here figure 4 is showing the analysis of the proposed WPAN network communication under the mobility variation. The horizontal labels are showing the scenario names and the mobility speed. The communication packet delivery ratio is shown in the figure. The figure shows that as the mobility is increased in the network, the packet delivery rate is improved.

V. CONCLUSION

In this paper, an optimization to the WPAN communication is provided based on the parametric evaluation. The method is defined to consider the network load and energy constraints to generate the effective network path to the infrastructure devices. The work is simulated in NS3 in different scenario. The results show that the effective communication throughput is obtained with lesser communication loss.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

REFERENCES

[1] Qingzi Liu, Qiwu Wu and Li Yong, "A hierarchical security architecture of WPAN," Cyberspace Technology (CCT 2013), International Conference on, Beijing, China, 2013, pp. 6-10.

[2] A. A. Wagan, B. M. Mughal and H. Hasbullah, "WPAN Security Framework for Trusted Grouping Using TPM Hardware," Communication Software and Networks, 2010. ICCSN '10. Second International Conference on, Singapore, 2010, pp. 309-312.

[3] L. Bariah, D. Shehada, E. Salahat and C. Y. Yeun, "Recent Advances in WPAN Security: A Survey," Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd, Boston, MA, 2015, pp. 1-7

[4] I. K. Azogu, M. T. Ferreira, J. A. Larcom and H. Liu, "A new anti-jamming strategy for WPAN metrics-directed security defense," 2013 IEEE Globecom Workshops (GC Wkshps), Atlanta, GA, 2013, pp. 1344-1349.

[5] M. Prabhakar, J. N. Singh and G. Mahadevan, "Defensive mechanism for WPAN security in game theoretic approach using heuristic based ant colony optimization," Computer Communication and Informatics (ICCCI), 2013 International Conference on, Coimbatore, 2013, pp. 1-7

[6] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer and B. Eissfeller, "Emerging attacks on WPAN security based on GPS Time Spoofing," Communications and Network Security (CNS), 2015 IEEE Conference on, Florence, 2015, pp. 344-352.

[7] A. A. Wagan, B. M. Mughal and H. Hasbullah, "WPAN security framework for trusted grouping using TPM hardware: Group formation and message dissemination," 2010 International Symposium on Information Technology, Kuala Lumpur, 2010, pp. 607-611.

[8] L. Chen, H. Tang and J. Wang, "Analysis of WPAN security based on routing protocol information," Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on, Beijing, 2013, pp. 134-138.

[9] Hongyu Jin and P. Papadimitratos, "Scaling WPAN security through cooperative message verification," Wireless Personal Area Networking Conference (VNC), 2015 IEEE, Kyoto, 2015, pp. 275-278.

[10] G. Yan, B. B. Bista, D. B. Rawat and E. F. Shaner, "General Active Position Detectors Protect WPAN Security," Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on, Barcelona, 2011, pp. 11-17.

[11] J. J. Haas, Y. C. Hu and K. P. Laberteaux, "Real-World WPAN Security Protocol Performance," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, Honolulu, HI, 2009, pp. 1-7.

[12] I. K. Azogu, M. T. Ferreira and Hong Liu, "A security metric for WPAN content delivery," Global Communications Conference (GLOBECOM), 2012 IEEE, Anaheim, CA, 2012, pp. 991-996.

[13] A. A. Wagan and L. T. Jung, "Security framework for low latency WPAN applications," Computer and Information Sciences (ICCOINS), 2014 International Conference on, Kuala Lumpur, 2014, pp. 1-6.