Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July 2021: 5205-5218

An Analysis of Data Transmission by using Wireless Personal Area Network for Improving Communication Throughput

Abhishek[1], Dr. Vaibhav Jain [2], Dr. Pawan Kumar[3], Dr. Pankaj Gupta[4], Dr. Deepak Goyal [5]

[1]M.Tech Scholar, Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak, abhishekyadav892987@gmail.com

[2]Assistant Professor, Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak, vaibhav_apr30@gmail.com

[3]Assistant Professor, Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak, pawankr8732@gmail.com

[4]Professor, Department of Computer Science Engineering, Vaish College of Engineering, Rohtak, pankajgupta.vce@gmail.com

[5]Professor, Department of Computer Science Engineering, Vaish College of Engineering, Rohtak,

deepakgoyal.vce@gmail.com

Abstract

WPAN is the wireless network defined in limited personalized area. The mobile nodes are defined with specification energy and the coverage restrictions. In this work, a route formation method based on connectivity, load and energy analysis is provided to improve the strength of network communication. The rule is applied on each immediate node to verify the strength of next communicating node. This analysis is applied on each node between source and the destination. The proposed work model is implemented in NS3 environment. The simulation of work is implied on five different scenarios. The work shows that the method has provided the significant throughput. The network is analyzed in terms of network size and the mobility. The results show as the mobility in the limited coverage is increased, it can result the higher communication loss and lower packet delivery ratio. The area based analysis shows that the communication loss is increased for lower network area. The lower density in the network increased the network throughput.

Keywords: WPAN, Communication, Network, Througput

1. Introduction

A Wireless Personal Area Network is the adhoc network defined without specification of any specialized controller or infrastructure. The dynamism is the main feature of this network form available in different forms. These kinds of networks are basically defined to provide high level cooperative communication between the pair of vehicle nodes which can be available at different geometric locations. This heavy communication is drawn using larger data files, video files or the transaction files. As the security is the main criteria, such kind of network requires the high speed communication with higher reliability. Because of this these networks are suffers from heavy

communication load. The communication links for this network under cooperative node identification. The communication can be controlled using different network architectures including the indoor network architecture, outdoor architectures, hybrid architectures etc. The dedicated network requires the direct transition between the network elements or the nodes so that the fast and safe communication will be obtained from the work. The content level communication analysis is defined by this network to observe the node level and network level communication. To provide high communication, the network requires the high bandwidth. The long distance communication is also the basic requirement of this network form. The communication or the transition in the network is also controlled using different constraints specified. In biometric application, big data processing, video communication are the common application areas of such networks. This network form also provides the internal communication observation with cooperative node identification and the control. The communication support is here provided at multiple mode as well as for single mode. The core diameter specific communication can be drawn through the communication links. The parmater driven analysis with cooperative connecitivty is applied and observed. The communication distance, communication media and technology are the other parameter which can control the communication so that the effective communication will be drawn. Some basic properties of this switched network is given here under

1.1 Data Transmission Types

The communication in the mobile technology can be performed with specification of IP Address. This kind of communication enables the dedicated end to end communication with involvement of lesser number of intermediate nodes. The network can have multiple network nodes so that the effective data communication can be performed. The communication is here been controlled by specification transportation layer protocol. The data type specification with connection oriented communication is defined. Based on the requirement, the connection specific or the connection less communication can be drawn over the network. To control the communication, the routing protocol can be defined. The infrastructure specific communication can be drawn to generate the effective communication path so that the technology enabled path will be obtained.

1.2 Communication Architecture

A switched network is having multiple constraints relative to the comunicaiton, architecture and the protocols. The communication can be drawn by involving some major technological terms in the network including the WPAN, frame relay communication the VAN (Virtual Area Nework). The frame relay specific communication can be drawnwith cell specification. The communication control method with the cell specification can be defined for effective communication control. The method driven estimation and the header value based differential estimation is also the key vector relative to this work. The node level specification is required to provide the cooperative links between the nodes. The communication can be of fixed or the variable size packets. The network cause to the lable is defined it this stage so that the controlled communication will be drawn. The ingress label edge routing method is ehre defined to provide the effective communication. The communication technology requires a specific control for reliability driven communication. The error checker and the maintenaince phases are also provided in this stage to minimize and mitigate the communication loss. The communication control with data packet specification is done. The source, base and size the

key vectors defined while enabling a communication. The communication can be enabled with specification of the technology so that the core network can be observed with routing table formation. The communication is here performed through dedicated wired links. The level based network is been suggested in this architecture.

As the communication is performed, the unicast or the multicast communication can be performed by specification of the label of the dedicated communication switches. The communication capabilities, the processing capabilities and the communication constraints are also defined to enable the communication and to provide the controlled communication over the network. The network infrastructure is one of the major aspect of this communication network. The network includes the control and the data unit to provide the communication and the control methods. The communication observation is also applied through the switch and the routing devices. The packet level and the label driven communication is performed over the network at higher speed. The unused communication links can be generated to avoid the situation of congestion or the bottle neck. The network fault can occur in some cases because of which some backup communication or the recovery method is required. The maintenance stage is required to provide the controlled communication over the network.

1.3 IEEE 802.11

This protocol defines the single MAC that interact with three PHY under frequency hopping and spread spectrum with 2.4 GHz band, direct sequence based spread spectrum in 2.4 GHz band and the infrared communication. This MAC protocol provides the distributed coordination function and point coordination function. This protocol standard defines the MAC layer.

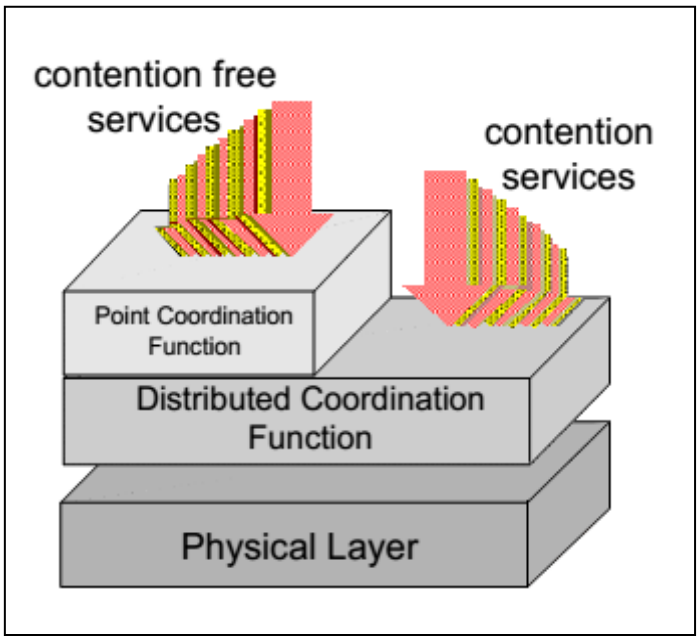

Fig.1: IEEE 802.11 Architecture

Here MAC layer is responsible for two type of communication services. The first service is contention free service which is provided by distributed coordination function. Another kind of service provided by MAC layer is contention free service implemented by the Point Coordination

function. These services are available at top of physical layer. The communication is here provided under three different communication standard called Infrastructure, FHSS (Frequency Hoping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum)[3][4].

2. Literature Survey

Bariah et. al.(2015) has explored the different features and aspects of vehicular security. Author identified the structured and comprehensive observation on different security aspects. The exploration to available security services, security constraints relative to different threats is provided by the author. Author also identified the security assessment tools and relate them to the security requirements. Author identified different attacks and the relative incentives so that the key driven communicaiton will be performed. Author also provided the detailed description of different simulators for WPAN including the NS2, Glomosim etc. Different scenario generation models were also provided by the author [3].

Bittl et. al.(2015) has provided the GPS based vehicle tracking in secure communication integration to provide the safe communicatioin against the emerging attacks. Author provided the attack preserved analysis to provide the network reliazation against the DOS attack. The repudiation feature of the security model also generated the pre observation on nodes against sybil attack. The preventive measure is here defined to outline the security flaws and setup the possibility against different attacks. The time stamp analysis is also provided by the author to provide the secure communication. The local time and multiple independent time based analysis was also provided to generate the safer communicating nodes. The safety critical observation over the vehicle nodes was provided to generate the secure featured communication in Wireless Personal Area Network [6].

Chen et. al.(2013) has defined an analytical security model for improving the communication in Wireless Personal Area Network. A feature level characterization was provided by the author with topological structure specification. The security challenge relative to the network was handled by the WPAN under four different category. The content based analysis was provided to generate the safe network communication. The topology and the position driven analysis was provided to generate the safe communication path. The directional information processing with transportation system was observed during the communicatio to improve the communication gain. The intrusion preserved communication was provided to generate the safe communicatio over the network. The protocol derived communication under the certain treatment was provided to achieve the selective routing [8].

Jin et. al.(2015) has improved the security scalaing for Wireless Personal Area Network by incorporating the cooperative message communication and verification. The method extended the security constraint by generating the message level verification at vehicle level. The message velidation and the message revocation was provided by the author to achieve the effective communication against the misbehavior analysis. The adversary model is here defined under cooperative verification so that the signed message communication will be performed. The hash function based malicious communication was provided with verification and checking. The probability adpative misbehavior analysis was provided to observe the neighbors so that the adpative cooperative communication is performed. The malicious node based probability analysis is provided to generate the vulnerability analysis so that the harmless analysis is provided. The prior

optimization was integrated to improve the reliable communication in Wireless Personal Area Network [9].

Wagan et. al.(2014) introduced a new low latency based security framework for enhancing the communication reliablity in Wireless Personal Area Network. The security integration was here defined with specification of cryptographic schemes including the asymmetric PKI and symmetric key based communication. Author improved the secure data exchange with key specification to achieve the critical communication safety. The trust enhacement was proposed by the author to achieve the trust adpative communication in Wireless Personal Area Network. The group entity specification was here defined with generation of cell and segments so that the group based communication will be performed. The symmetric key exchange based data communication was provided by the author. The group leader based based and reliable V2V communication was provided by the author [13].

Sumra et. al.(2015) has provided a work on trust and privacy analysis to achieve the secure and reliable communication in Wireless Personal Area Network. The proposed method has generated a hardware oriented card based scheme to achieve the communication trust and security. The environment specific potential secure communication was provided by the method. This method provided the user level, location level and route level security. The security was here provided in terms of annoymous attestation and the certification at node level [15].

Varshney et. al.(2014) has defined a digitial certification method using the bandwidth specific estimation and providing improved security mechanism for Wireless Personal Area Network. The process is here defined to achieve the secure communication between the vehicles and the infrastructure. The attack specific analysis was provided to identify the secure message passing with reduced communication bandwidth. The protocol integrated security was provided with lesser computational cost and improved performance measures. The algorithmic specification was provided to generate and distribute the certificates as well as to control the communication [18].

Ahmed et. al.(2015) has defined a layered method for improving the WAVE security in Wireless Personal Area Network. The security model provided here was divided in differet domains. At first level the region transportation authority based key generation and management was provided. Later on the RSU role is defined to turn and store the keys and information. The access point verification and authentication was also provided by RSUs. The vehicle level encoding and decoding was done using the symmetric key cryptography method. The message level priortization ensures the consitent and secure communicaiton in Wireless Personal Area Network [20].

3. Methodology

3.1 Research Objectives:

The objectives associated to this work are listed below:

- The main objective of work is defined to provide the effective node discovery under multiple load and communication parameter analysis.

- The objective of work is to generate the rules for effective neighbor selection and present it as intermediate nodes.
- The objective of work is to implement the work in NS3 environment
- The objective of work is to improve the communication throughput and reduce the communication delay.

3.2 Working with WPAN:

WPAN is the technology driven network to provide the broadband access to the network. The access services so that the enterprises and economic specific communication can be performed. WPAN is the standard network form so that the standardized network form is defined. The alternate communication respective to the broadband access is available in the critical network scenario. Various industries, institutions use this network form for component level node tracking. The interoperability to network form is provided to achieve the effective access to the broadband network. A WPAN system consists of two major parts:

- A WPAN base station.
- A WPAN receiver.

The limited network is defined with fixed base station in the personalized network. The smaller base stations or the cover towers are established to capture the communication to provide the communication support and interoperability in the network system. The switching among these base stations can be done under mobility. The bandwidth specific communication and the reliable incooperated communication is performed. The real time communication can be established through the uplink and downlink specific bandwidth specification.

3.3 Communication Modelling

GPSR Enabled Tracking is a fundamental issue in a Wireless Personal Area Network, which determines how well a phenomenon of interest i.e. Vehicle Devices is monitored or tracked by GPS controllers.The GPS Enabled Tracking concept is the measure of the Quality of Service (QoS) of the sensing function and is subject to a wide range of interpretations due to large variety of GPS devices and applications. The goal of GPS Enabled Tracking is to have each location in the physical space of interest within the sensing range of at least one GPS enabled Vehicle device. Additionally the GPS Enabled Tracking formulations try to find the weak points i.e. the points which are least covered by the GPS enabled devices in a sensor field and suggest future deployment and reconfiguration schemes for improving the GPS Enabled Tracking performance. Generally the GPS Enabled Tracking involves the two basic ideas [5]:

- The evaluation of GPS Enabled Tracking performance when the Vehicle nodes are deployed in the monitoring region.
- The improvement of the GPS Enabled Tracking performance when the vehicle network cannot effectively satisfy the application requirements.

The GPS network is able to provide the tracking of the mobile nodes in the coverage area. These devices are defined relative to the base station and the region specification. The sensing or the coverage area is also defined for tracking of the node. The node level location tracking and monitoring can be done on the distributed nodes for classification of the nodes based on the coverage observation. The failure of the nodes can be obtained in the coverage if the communication failure occur in the network form. The tracking of the nodes can be done based on the degree level analysis. Each node track the information of neigboring nodes by detection of the sensing specific positional observation. The GPS enabled sensors are defined to cover the region so that the location specific communication with the coverage can be performed. The coverage can be formulated so that the identification of active nodes can be done. The controller specific observation can be performed so that the network region tracking can be obtained in the system. The controller device specific observation is done to minimize the network communication. The effort estimation can be done and for this the log information is recorded and maintained in the network.

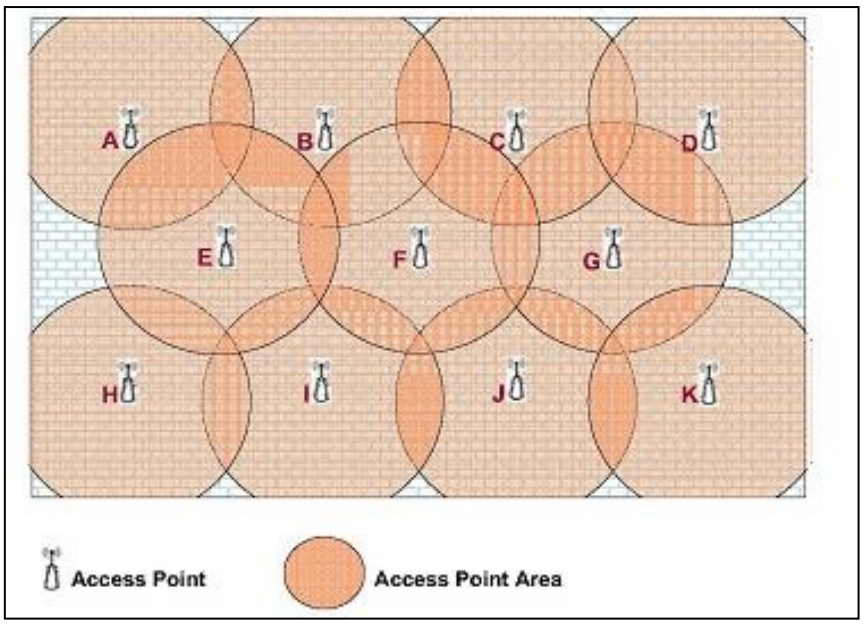

Fig.2 : GPS Controller based tracking

The coverage is the main problem in the personalized network because of existence of the obstacles or walls and the placement of the base station. The node level tracking in the area is required specific to the node and the base station. The GPS devices specific nodes are distributed in the network so that the tracking can be done based on the regional coverage. The limited sensing based node deployment can be performed so that the energy adaptive communication can be performed. The sensing range is defined to provide the extensive node level mapping so that the regional updating and the switching to the base stations can be performed. The regional evaluation to the coverage can be obtained to achieve the maximum connectivity and to save the energy consumption in the network.

Location Log or Tracking

The formost tracking required here is for the actual physical location of vehicle node at particular time instance. this geographical position is the base estimator based on which the controller

identification will be done and relatively effective network communication will be performed. The coordinate specific information of vehicle node and relative mapping within the controller coverage region is defined. The distance estimation is performed for effective node tracking in the geographical region.

Movement Log

Another tracking of vehicle movement within the region is also defined in the network. The movement information processing and the movement path generation in the network is defined for the Wireless Personal Area Network. The location services and relative reference table is also generated for estimating the node position and generating the relative information track. In this work, the rule adaptive zone predictive measure is defined to estimate the pre-observation on node movement. This predictive tracking will provide the improvement to the referenced model so that the movement tracked communication will be performed.

Path Derived Communication

Once the relative controller to particular vehicle device is identified for a particular time instance, the next work is to perform the communication between the controller and the vehicle device. This controlled communication can be single hop or multiple hop based on which the packet transmission within network is obtained. The location specific services are here defined for tracking the node and providing the tracked communication. The agent specific and query specific communication can be defined for the registered vehicle nodes.

Featured Observation

While performing the predictive node tracking and communication, it is required to perform the controlled communication in the network. These parameters considered for effective node tracking are

- Fault Prediction
- Load

When the communication is applied, some communicatin effort estimation at different parameters will be derived. These parameters will include the network life estimation, network fault estimation etc. The comparative observation of the work model is also considered under the normal predictive measures as well as rule based zone predictive model. The integration of rules in the method also improved the computation strength of the proposed method and provided more accurate and predictive mapping to the vehicle nodes. The controller specific constraint mapping is here generated under the self organization map specification. These maps are based on the kinetic features of the network where the node tracking in generalized open environment is performed. The trackers are here defined within the network without specification of relative zone and the mapper specification. The tracker also enabled the controlled communication efforts in the network. The estimation at the higher level is been achieved in the network so that the predictive measurement at analytical parameters are obtained. The optimization is here required to provide the communication without communication of much battery and by reducing the communication fault. The proposed processed

stages associated to the work are defined in next stage. Later on the algorithm based on this predictive model is also defined.

4. Simulation Results

Scenario I:

In this work, a mobile network for WiFi network defined to simulate the work. The table is showing the simulation parameters.

Table 1: Simulation Parameters

Parameters	Values
Network Area	1000x1000
Number of Nodes	20
Protocol	AODV
Packet Size	512
MAC protocol	MACA
Topology	Random
Type of Network	WiFi
Simulation Time	1 Min
Mobility	400 to500m/s
Propagation	2 Ray Ground
Position	Random

Here table has showed the configuration parameter on the network scenario in which the WPAN network is established. The table is showing the physical constraints, communication constraints and the network level constraints. The network generation specific results are shown in this paper.

Analysis

Once the network is established and communication is performed, the next work is to perform the analysis on this network under different parameter. The mobility specific and the network density specific analysis is performed for the evaluation. The evaluation is done in terms of communication throughput, communication delay parameters. In this section, the node mobility specific observations are provided.

Mobility Based Analysis:

As the nodes present in the WPAN network are defined under the mobility in the limited coverage range. The parameters associated to this work are listed in table 2. Five different scenarios are generated based on different mobility level as shown in the table. Based on these parameters, the communication level analysis is taken and provided in this section.

Table 2 : Scenario Parameters

Parameters	Values
Network Area	500x500
Number of Nodes	10
Protocol	AODV
Packet Size	512
MAC protocol	MACA
Topology	Random
Type of Network	WiFi
Simulation Time	1 Min
Mobility	20 to 40 m/s for scenario I 30 to 70 m/s for scenario II 100 to 200 m/s for scenario III 10 to 90 m/s for Scenario IV 20 to 40 m/s for Scenario V
Propagation	2 Ray Ground
Position	Random
Communication Type	CBR, FTP
Parallel Communication	Yes

The table has defined the configuration constraint based on which the analysis is performed. The analysis is here done in terms of communication throughput, communication loss and the packet

delivery ratio. Based on this results are obtained provided in this subsection. The throughput based analysis is shown in figure 3

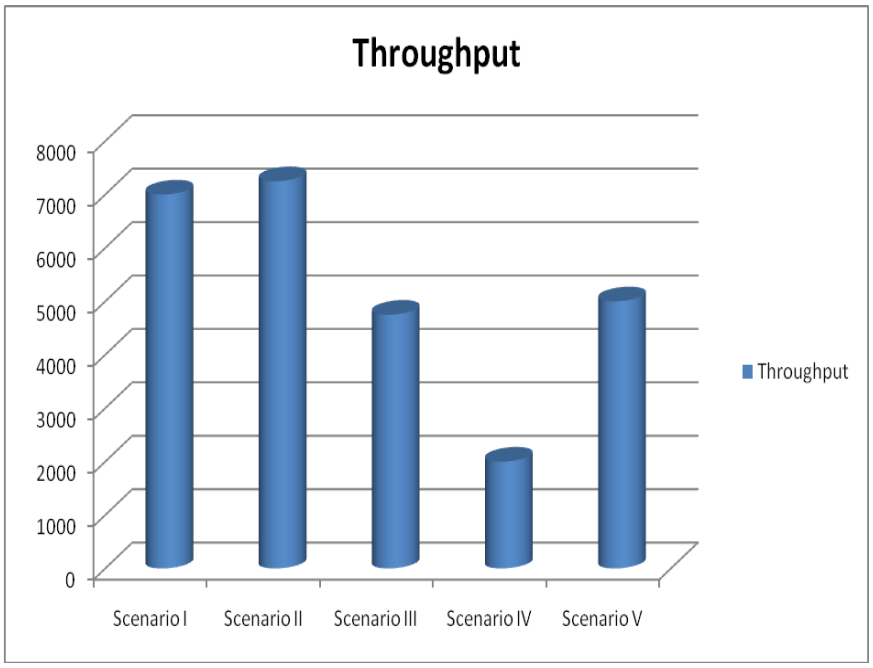

Fig.3 : Throughput Based Analysis (Mobility Variation)

Here figure 3 is showing the analysis of the proposed WPAN network communication under the mobility variation. The figure is showing the analysis on five different scenarios. The horizontal labels are showing the scenario names and the mobility speed of these scenarios is already shown in table 2. The figure shows that as the mobility is increased in the network, the communication throughput is decreased.

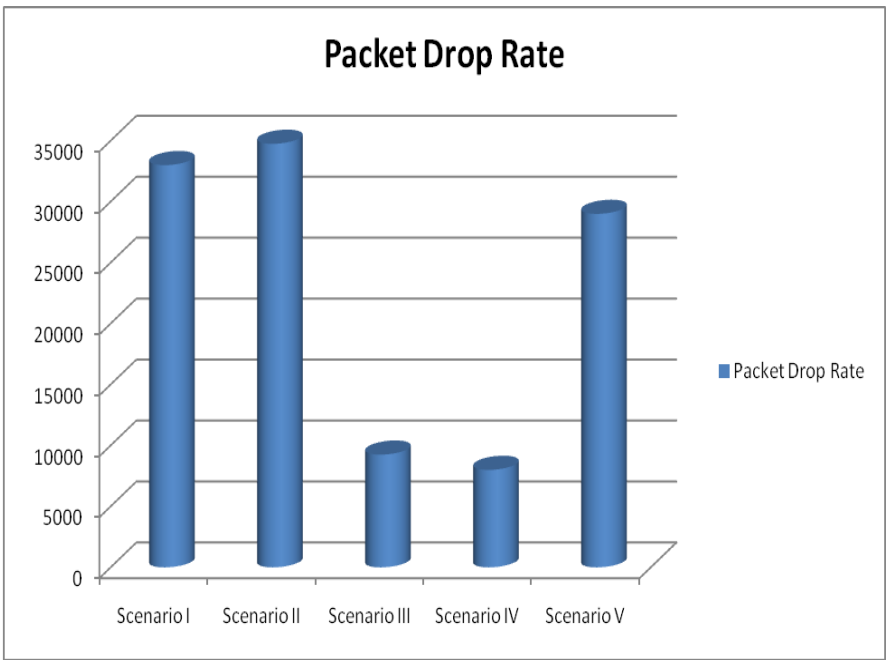

Fig.4 Drop Rate Analysis (Mobility Variation)

Here figure 4 is showing the analysis of the proposed WPAN network communication under the mobility variation. The figure is showing the analysis on five different scenarios. The horizontal labels are showing the scenario names and the mobility speed of these scenarios is already shown in table 2. The communication throughput is shown in the figure. The figure shows that as the mobility is increased in the network, the communication loss rate is increased.

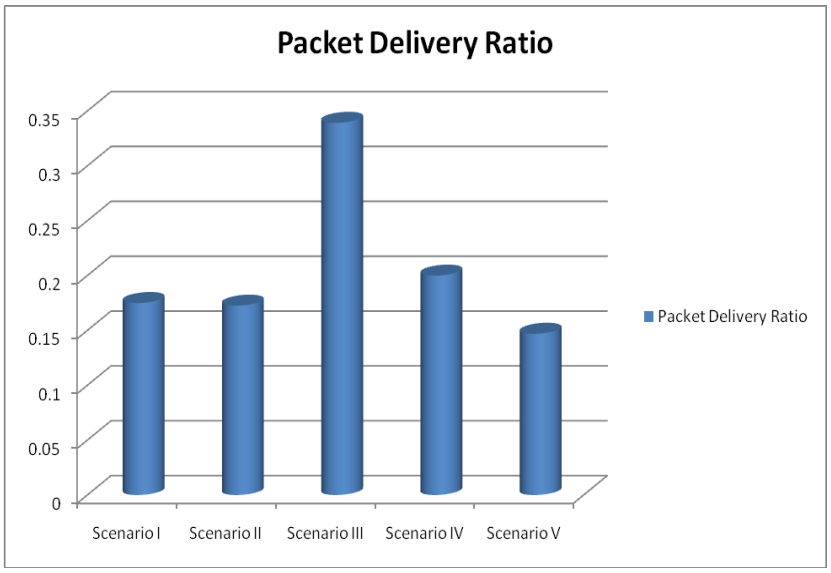

Fig.5 Packet Delivery (Mobility Variation)

Here figure 5 is showing the analysis of the proposed WPAN network communication under the mobility variation. The figure is showing the analysis on five different scenarios. The horizontal labels are showing the scenario names and the mobility speed of these scenarios is already shown in table 2. The communication throughput is shown in the figure. The figure shows that as the mobility is increased in the network, the packet delivery rate is improved.

5. Conclusion and Future Scope

In this work, an optimized communication to the personalized area network is provided by establishing the base station and the GPS enabled localized communication. The network model is based on the statistical communication approach to identify the effective route between the node to sub stations. The work can be extended in future under following aspects

- In this work, WiFi adaptive GPS tracking is provided to optimize the WPAN communication. In future, some other network technology such as WiMax can be used to improve the network communication.
- The work is defined on the personalized network, in future other network forms such as sensor network or vehicular adhoc network.

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.
14. R. V. Alexandrescu, M. C. Surugiu and I. Petrescu, "Study on the implementation of protocols for providing security in average WPAN intervehiculary network communication systems," Electronics, Computers and Artificial Intelligence (ECAI), 2015 7th International Conference on, Bucharest, 2015, pp. WW-1-WW-6.
15. I. A. Sumra, H. B. Hasbullah and J. l. A. Manan, "Using TPM to ensure security, trust and privacy (STP) in WPAN," Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on, Riyadh, 2015, pp. 1-6.
16. S. J. Horng; S. F. Tzeng; T. Li; X. Wang; P. H. Huang; M. K. Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in WPAN," in IEEE Transactions on Vehicular Technology , vol.PP, no.99, pp.1-1
17. B. Aslam and C. C. Zou, "One-way-linkable blind signature security architecture for WPAN," 2011 IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2011, pp. 745-750.
18. N. Varshney, T. Roy and N. Chaudhary, "Security protocol for WPAN by using digital certification to provide security with low bandwidth," Communications and Signal Processing (ICCSP), 2014 International Conference on, Melmaruvathur, 2014, pp. 768-772
19. G. Samara, W. A. H. Al-Salihy and R. Sures, "Security Analysis of Vehicular Ad Hoc Nerworks (WPAN)," Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on, Kedah, 2010, pp. 55-60.
20. K. J. Ahmed, M. J. Lee and J. Li, "Layered scalable WAVE security for WPAN," Military Communications Conference, MILCOM 2015 - 2015 IEEE, Tampa, FL, 2015, pp. 1566-1571.
21. G. Samara, W. A. H. Al-Salihy and R. Sures, "Security issues and challenges of Vehicular Ad Hoc Networks (WPAN)," New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on, Gyeongju, 2010, pp. 393-398.
22. M. Feiri, J. Petit, R. K. Schmidt and F. Kargl, "The impact of security on cooperative awareness in WPAN," 2013 IEEE Wireless Personal Area Networking Conference, Boston, MA, 2013, pp. 127-134.

23. E. Bubenikova, J. Durech and M. Franekova, "Security solutions of intelligent transportation system's applications with using WPAN networks," Control Conference (ICCC), 2014 15th International Carpathian, Velke Karlovice, 2014, pp. 63-68.
24. V. S. Chetan, N. S. Benni and C. Bhushan, "Security framework for WPAN for privacy preservation," Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on, Tiruchengode, 2013, pp. 1-6., 2015, pp. 1-6.