End to End VANET/ IoT Communications A 5G Smart Cities Case Study Approach

Melvin Hayes[1] and Tamer Omar[2]
Department of Technology Management, Indiana State University Terre Haute [1]
Department of Electrical and Computer Engineering, Cal-Poly Pomona [2]
Email: mhayes8@indstate.edu[1], tromar@cpp.edu[2]

***Abstract*—This paper investigates the infrastructure to vehicle and infrastructure to cloud connectivity and reliability in the vehicular ad hoc networks (VANET) area of Intelligent Transportation Systems (ITS). A key focus of this work is to investigate protocols that will enhance real-time, robust and reliable communication methods, and complement autonomous vehicles' navigation experiences within smart cities. The main areas of study include highway infrastructure that include the Wireless Sensor Networks (WSN) to the Cloud (web service) and vice-versa. The pertinent cloud-based data will be communicated to subscribed vehicles (with password access) to complete the V2I and I2V communication cycle. The data collected from the WSN is communicated to the cloud via XML over XMPP, zero configuration, and mDNS protocols. The use of the XMPP protocol to communicate data to the cloud data repository represents a novel approach to IoT harmonization for this particular infrastructure to cloud/I2V application.**

***Index Terms*—5G, Zero Configuration, MultiCasting Domain Naming Service (mDNS), XMPP, IoT Harmonization, TEDS, IEEE1451.**

I. Introduction

The area of Internet of Vehicles (IoV) is showing more interest form both academia and industry as more advantages are expected form such network. IoV include multiple aspects that guide the relation between the vehicle and the infrastructure and vice verse (V2I/I2V), and the relation between the different Autonomous Vehicles (AV), semi autonomous and non autonomous vehicles which is known as (V2V). This work aims at designing, testing and validating a Wireless Sensor Network (WSN) model for Smart Cities that will provide Real-time traffic monitoring. The model aims at providing early warnings from an active, robust, sustainable and secure system that will act as a Road Side Unit (RSU) sensor network which will operate as an Internet of Things (IoT) application.

Currently the industry is researching and investing in fifth generation broadband networking (5G) and its role in supporting IoT applications. These industries includes manufacturing, educational institutions, pharmaceutical industries, medical center , military, and transportation industry researching in the future of autonomous vehicles. This work seeks to investigate the robustness, availability, reliability, and security of adopting Extensible Messaging and Presence Protocol (XMPP) and open standard for messaging and presence protocol, the Multicast Domain Name System (mDNS) protocol, IEEE1451.7 and IEEE1451-99 a set of smart transducer interface standards in achieving end-to-end communications for IoT datum and meta-data collection and dissemination platform for IoV.

Furthermore, this work highlights and investigates the role that Zero-Configuration a set of technologies that can automatically creates a usable RSUs network based on the Internet Protocol Suite to support the proposed end to end communications systems design. This work is predominately interested in the upper layers of the data communication protocols for the Internet of Things (IoT) harmonization of WSN devices that can be used for a Vehicular Ad-Hoc Network (VANET) seamless metadata collection and dissemination. V2I and V2V technologies has not fully developed to Level that allow long term sustainability, robustness and scalability. With secure IoT algorithms and protocols the 5G and IoT harmonization protocols and techniques to can be adopted, adapted and implemented for maximum IoV efficiency and safety.

This study aims at identifying the inefficiencies and ineffectiveness of VANET communications and evaluated methods to effectively manage them.The work also investigate ways to increase the throughput of VANET communications, exploring what can be done to increase the Security of VANET against cyber-attacks and hacking, and finally to contribute to the ways that the can utilize IoT networks by designing and managing an scalable network that work in harmony for the betterment of society.

Figure 1 shows one of many arrangements for the Wireless Transducer Interface Modules (WTIM) that can be used for WSN data collection and dissemination [1]. Authors in [2] demonstrated how the IEEE1451.7 standard can be used as a transducer layer protocol to retrieve data from a WSN which may act as a RSU within a WSN design for V2I/I2V and Vehicle to Cloud (V2C) design scenarios or schemes. This research provides more detail about the operations of the intermediate layers of the architecture in the system design. This layer is responsible for the integration between the transducer layer where AV system control is performed and the cloud system where the ITS takes place. This layer is implemented inside the RSUs using latest wireless technologies and secured communication systems This research also shows that through emulation, data collection, and simulation that a 5G compliant, IEEE1451-99 compliant WSN data collection and dissemination network can be made viable and cost effective with today's technologies.

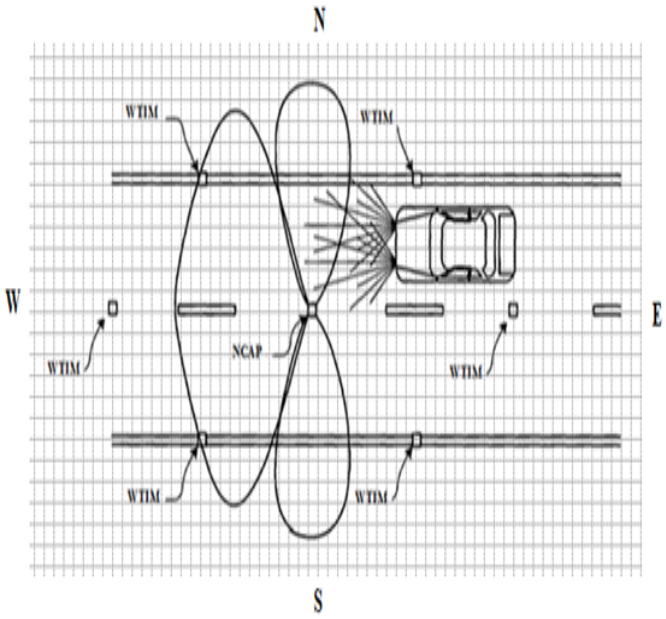


Figure 1: Network Topology

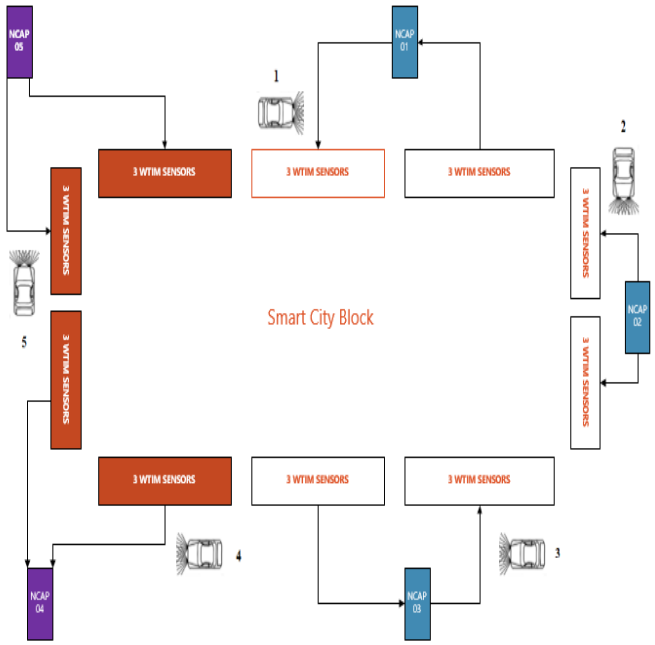


Figure 2: Network Topology

II. System Architecture & Design

A. Network Topology

Figure 2 represent a sample network topology for the proposed solution. The topology represents a V2I sensor coverage for a Smart City block of (660 ft x 920 ft). The proposed solution adopt both IEEE1451-99 in the sensors/transducer level and XMPP for secure communication of any required parameters using embedded transducer electronic data sheets (TEDS). Authors in illustrated in [3], [4] how the IoT Harminozation (IEEE1451-99) can best be achieved and implemented using the XMPP protocol. The author describes how the XMPP protocol can address the four communication patterns and bridge the various protocols that exists by connecting the isolated computers, laptops, cellphones, and tablets that are in use today. Three of the predominant four patterns that are in common use today and have already been addressed by the XMPP protocol were identified as follows

1) Asynchronous messages.
2) Request/Response services
3) Publish/Subscribe mechanism.

XMPP has native support for the above three patterns through the message, iq and presence stanzas, which are the name for packets being transmitted in the XMPP network. A Stanza expresses an entity's of current network availability and in our case it expresses the availability of a certain vehicle in the IoV.

The presence stanza supports persistence of the last content published and confirm that a second Publish/Subscribe method with more persistence options is available in XEP-0060 [5], also Multi-casting for multiple recipients is available through XEP-0045 [6]. XMPP protocols allow simple bridging of information using any of the well-known and well-used communication patterns available and steps to make these patterns standardized. XMPP uses a Publish/Subscribe mode, where publishers publish information to a broker, which publishes it, and later distributes it to a negotiated set of subscribers.

The work in [7] indicated that with mDNS and DNS Service Discovery (DNS-SD) protocols, a user-friendly and seamless discovery of smart objects can be implemented. Multicast DNS (mDNS) protocol is part of a group of standards that are used to automatically enable computers to look for or find other devices and to share their services with each other in network environments without manual configuration by the user[8].

The task of mDNS protocol is to resolve domain names without the help of any unicast DNS server by delivering messages to the reserved multicast addresses 224.0.0.251 (IPv4) and ff02::fb (IPv6) via UDP port 5353. Devices inquire network addresses with requests to a multicast group. The respective device responds with its list of DNS resource records. The mDNS protocol is often implemented together with DNS Service Discovery (DNS-SD) protocols. The two are available for various platforms, such Mac operating system (iOS) and Windows with Bonjour , and for Linux, BSD, OpenWRT, and Android with Avahi.

The DNS-SD protocol is another part of the standards used to discover devices and share their services. It is combined with the mDNS protocol and also supported by the Bonjour and Avahi protocols. The DNS-SD protocol enables the location and announcement of services to entities in a network domain. DNS resource records are again used to provide information about services. Authors in "Chatty Things"[9] mentioned that XEP – 0174 allows two entities to establish an XML stream without the need of a XMPP server while using the mDNS and DNS – SD protocols to discover entities that support XMPP and to indentify their IP addresses and preferred ports, using the _presence._tcp DNS SRV service

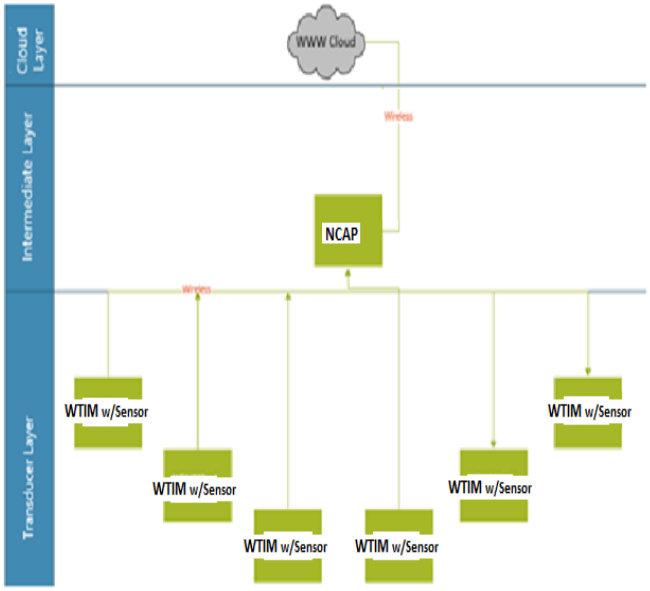


Figure 3: Three Layer Architecture

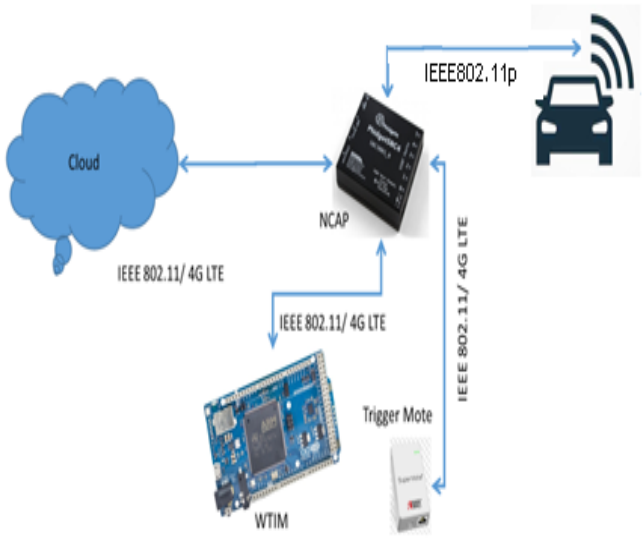


Figure 4: System Design

type.

Figure 3 represents one of the architectures that were investigated by our team in a smart city case study presented in [2]. This design covered a wider and longer area than a smart city block to allow model generalization. As shown the architecture include three layers:

1) Transducer Layer: presents the different RSUs equipped with Wireless Transducers Interface Modules (WTIM) with the required sensors.
2) Intermediate Layer: presents the central Network Capable Application Processor (NCAP) that relay the messages from the transducer layer to the cloud layer.
3) Cloud Layer: hosting the Intelligent Transportation System (ITS) used for traffic conditions analysis and optimization.

III. System Design & Preliminary Results

In order to accomplish end-to-end communications using the three layer model, a different transceiver device is used at each end of the system design. One of the transceivers devices represented the Infrastructure of the V2I/I2V system. The second transceiver (Samsung smartphone) represented the vehicle or cloud part of the I2C/C2I system. Figure 4 shows the cloud computing hardware, software (control and sensing), RFID transducers using TEDS for read/write operations can be used to implement the proposed architecture. In order to simulate the designed system and use XMPP messages to communicate the TEDs between the WTIMs and the cloud a test-bed was used to examine the proof of concept.

For implementation purposes the test bed used a Samsung Galaxy Tab Tablet with 4G WiFi SM-T285 8 GB as local end device for short range communication data collection testing. This device used to emulate a mote or WTIM with embedded sensors and using WiFi technology for data collection and data dissemination to the NCAP module or to a matched NCAP module. This device was loaded with the Yaxim smartphone application, the Yaxim operates using XMPP protocol as software/middleware to provide end-to-end IoT Harmonization at the Transducer layer of our system model design.

In addition to the above equipment, a Samsung Galaxy S5 smartphone is used with 4G LTE capabilities to represent long range communication data collection case. The smartphone and accessories were loaded with the Yaxim software application in order to communicate with the Samsung A6 tablet using XMPP in end-to-end communication. In this work, the Samsung smartphone represented a licensed/approved Vehicle of our I2C and I2V data collection design.

Three sets of datum was taken from three testing locations to emulate the vehicle movement. These datum were taken at the same time of day on two different days of the week. The three locations that were used for the data-sets mentioned above are:

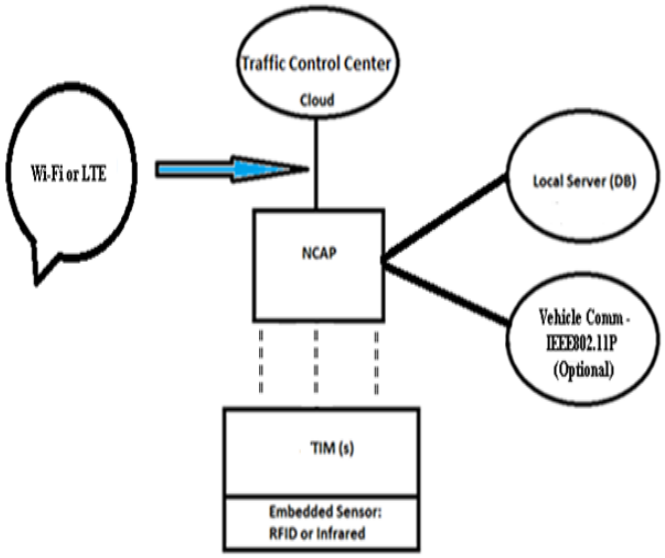
1) Location 1 (Office/Lab).
2) Location 2 (Tim's House).
3) Location 3 (Robert's House).

The three messages that were sent for testing are:

1) Initial message of "Hello Today".
2) A second message that reads "Nice Photo".
3) The second message has an attachment of a colorful "Caribbean Parrot" of about 3.28MB.

The steps followed in data packets collection, organization, and analysis are as follows:

1) Separate messages are sent between WTIM-NCAP using secured XMPP protocol.
2) The messages sent are intercepted and observed via Wireshark from three separate locations.



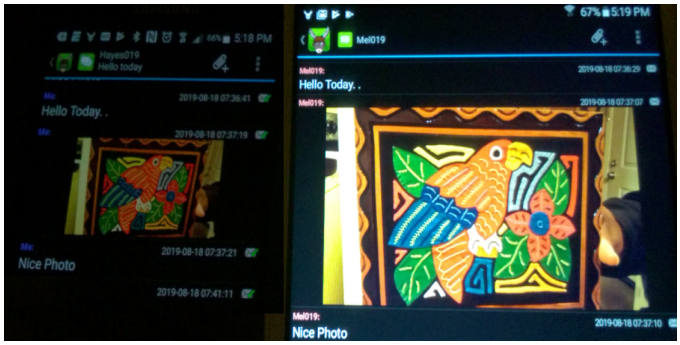
This XMPP model Architecture requires only one hop from NCAP/TIM sensor module to local DB or Cloud DB.

Figure 5: XMPP Model

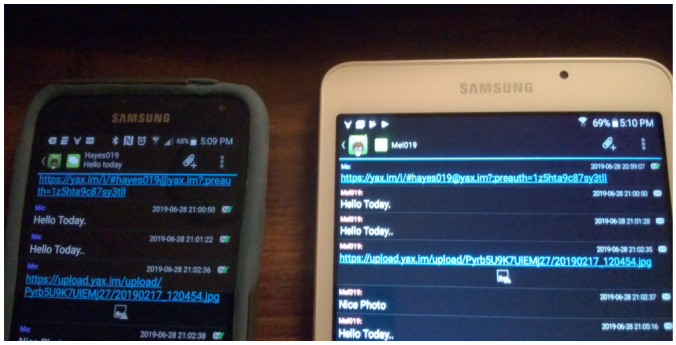
3) Collected data placed into spreadsheets for further statistical analysis and organization to validate the reception of the sent messages.

Figure 5 represents the XMPP model used for communicating the TEDS in the current system design. The figure explain the communication model and the role of XMPP in TEDs transfer. The WTIMs uses IEEE1451.7 and IEEE1451-99 smart transducer interfaces to communicate to the vehicle and collect the required TEDs by the ITS. The data is relayed from the WTIMs using a second WiFi interface to the NCAPs, this support the work in a free licensed spectrum in addition to increase the coverage area between the WTIMs and the NCAPs. Additionally, TEDs will be transmitted to the ITS located in cloud using 4G LTE technologies. The proposed solution can take two approaches, either centralized approach by directly relaying the TEDs to the ITS or by using a distributed approach. The distributed approach will store the data locally in the NCAP using a database service and then relay the data according to fixed schedules. It is also possible for vehicles that support WiFi based WTIMs to send its TEDs to the NCAP using any supported IEEE 802.11 technologies. Finally the TEDs can be collected, organized, and analyzed by the ITS that can use this data to optimize the traffic conditions by sending recommendation to the AVs such as alerts, traffic congestion, work zones or more advanced route changes.

Figure 6 shows the text and photo transmission and receipt between our two experimental data collection devices. The figure also shows the original text information with time stamp for two messages and the 3.28MB photo with time stamp that we used as our platform for data transmission, collection and protocol and packet capture and analysis. The words “Hello Today” and “Nice Photo” are brightly readable in the Upper right and lower right corners of the right half of the figure.



(a) Transmitted Text and Photo



(b) Yaxim XMPP Messages

Figure 6: Data Transmission

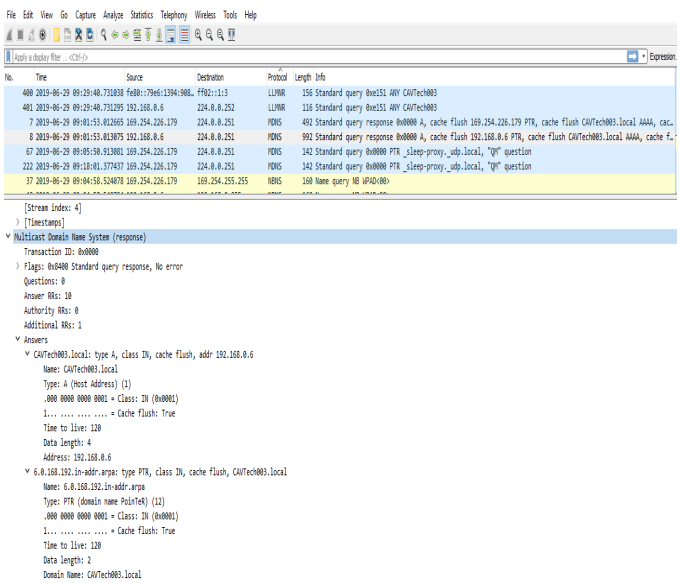


Figure 7: Packet Analysis

Figure 7shows WireShark packet capture for analysis and statistics purposes. Wireshark packet analysis software tool is used to capture and analyze the XMPP protocol packets created each time that a communication transaction is executed between the two communication devices [10]. A legacy Dell Optiplex 745 desktop computer is use to sniff the traffic and capture the wireshark data as it moved from the smartphone 4G LTE and WiFi platform to the tablet in location 1 via the broadband router used end to end operations.

Future analysis for the captured traffic will be used to validate the secured XMPP messages communication. A primary finding indicates that the received XMPP messages may be encrypted during the communication path. However, to validate this finding two scenarios are planned to convert the send XMPP messages to plain messages and intercept them to ensure the cabability to identifying the messages using WireShark. Furthermore, encrypted XMPP messages if confirmed will be extracted from the wireshark traffic and Man In The Middle (MITM) Attacks will be examined to test the capabilities of attackers to manipulate the collected TEDs in a way to hack the ITS by providing false information.

IV. Conclusions

We were able to successfully send and receive data over the network using an XML over XMPP application for android systems. Our mDNS protocol data packets were captured and analyzed using the Wireshark packet analysis tool. No intrusive or hacking activity were detected within our data collection. However, we are continuing to evaluate the security and robustness of the zero configuration and the mDNS protocol packet traffic that we are using for our NCAP to Cloud data collection. More work is needed in filtering our packets for greater security, a more robust communications and to manage our impact on the available bandwidth at any given time.

From this research no intrusive or hacking activities were detected within our data collection. However, we are continuing to evaluate the security and robustness of the zero configuration and the mDNS protocol packet traffic that we are using for our NCAP to Cloud data collection. More work is needed in filtering our packets for greater security, a more robust communications and to manage our impact on the available bandwidth at any given time.

References

[1] E. Y. Song, K. B. Lee, S. E. Fick, and A. M. Donmez, "An IEEE 1451.5/802.11 standard-based wireless sensor network with embedded WTIM," in *2011 IEEE International Instrumentation and Measurement Technology Conference*, May 2011, pp. 1–6.

[2] M. Hayes and T. Omar, "An IEEE1451.7 Based WSN Design for V2I Localization Services in Smart Cities," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, Nov 2018, pp. 19–25.

[3] Peter Waher and Little Sister, "IoT Harmonization using XMPP: How XMPP can be used to interconnect isolated protocol islands." [Online]. Available: http://sensei-iot.info/PDF/IoT%20Harmonization%20using%20XMPP.pdf

[4] P. Waher, *Mastering Internet of Things*, 2018.

[5] Peter Millard, Peter Saint-Andre, and Ralph Meijer, "XEP-0060: Publish-Subscribe," XMPP Standards Foundation, 2017. [Online]. Available: https://xmpp.org/extensions/attic/xep-0060-1.15.0.html

[6] P. Saint-Andre, "XEP-0045: Multi-User Chat," XMPP Standards Foundation, 2017. [Online]. Available: https://xmpp.org/extensions/attic/xep-0060-1.15.0.html

[7] R. Klauck, "Seamless integration of smart objects into the internet using XMPP and mDNS/DNS-SD," Ph.D. dissertation, 05 2016.

[8] ——, "Seamless integration of smart objects into the internet using XMPP and mDNS/DNS-SD," Ph.D. dissertation, 05 2016.

[9] R. Klauck and M. Kirsche, "Chatty things - Making the Internet of Things readily usable for the masses with XMPP," in *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, Oct 2012, pp. 60–69.

[10] Sherri Davidoff and Jonathan Ham, *Network Forensics: Tracking Hackers through Cyberspace*. Pearson, 2012.