ITCP based Security Enhancement for IoT Devices in IPV6 Protocol

Shubhalika Dihulia
M.Tech Student
Department Computer Science Engineering
All Saints college of Technology, Bhopal, India

Tanveer Farooqui
Assistant Professor
Department Computer Science Engineering
All Saints college of Technology, Bhopal, India

ABSTRACT
In this paper, present an improved transmission control protocol. For IoT devices. Currently there are different protocols are exist based on user data gram approach. Similarly TCP is also worked alone, In this present work proposed and improved transmission control protocol that is the hybrid concept of TCP and UDP on IPV6 platform. In the ITCP protocol TCP is used for link connection between two devices and UDP is used for the data sending. On the basic on this proposed new protocol that shows good improved result the transmission time, throughput, packet delivery ratio and other parameters as compare to other IoT protocol present in the IoT. For the simulation of proposed ITCP protocol used JAVA platform. Also compare the proposed result with different protocols.

Keywords
Computational time, throughput, packet delivery ratio (PDR), packet loss, transmission control protocol (TCP) and User data gram protocol (UDP).

1. INTRODUCTION
The Internet of Things (IoT) is a very important topic within the technology business, politics, and engineering circles and have become headline news within the trade press and common media. This technology is incorporated into a large vary of network product, systems and sensors that cash in of advances in computing power, electronics miniaturisation and interconnection of networks to supply new options not antecedently attainable. A conference abundance, reports and press articles discuss and dialogue the potential impact of "IoT revolution" -to new market opportunities and business models to considerations regarding security, privacy and technical ability. [02]

The large-scale implementation of IoT devices guarantees to rework several aspects of however we have a tendency to live. For customers, the new IoT product like Internet-enabled devices, home automation parts, and energy management systems to guide us towards a vision of "smart home", providing larger potency and security Energy. alternative personal devices IoT devices as fitness and moveable health observation and medical device license network are reworking the approach health services area unit delivered. This technology guarantees to be useful for individuals with disabilities and also the old, thereby up levels of independence and quality of life at an inexpensive value. IoT systems as networked vehicles, intelligent transport systems and sensors embedded in roads and bridges bring us nearer to the thought of "smart cities", that facilitate to scale back congestion and energy consumption. The IoT technology offers the likelihood of reworking agriculture, business and also the production and distribution of energy by increasing the provision of data on the assembly worth chain victimization networked sensors. However, the IoT raises several problems and challenges that require to be thought of and addressed if the potential advantages to be complete.[10]

Some observers see the IoT as absolutely interconnected world revolutionary "smart" progress, efficiency, and also the ability, with the flexibility to feature billions important to the trade and also the international economy. Others warn that the IoT represents a darker world of surveillance, privacy and security breaches, and shopper lock-in. Attention-grabbing titles on piracy of Internet-connected cars, considerations arising from superior voice recognition options in "smart" TVs, and fears of privacy derivation from the IoT knowledge from potential abuse captured the general public attention. This dialogue "promise vs risk" and a flood of data that the popular media and promoting will create IoT a fancy subject to know.[4]

Basically, the web Society cares for the IoT, it represents a side more and more the method individuals and establishments are possible to move with the web in their personal, social and economic. If even modest projections area unit correct, explosion IoT applications might cause a elementary amendment within the manner users move with and tormented by the net, that raises new queries and also the completely different dimensions of the present challenges through the user/ shopper considerations, technology, politics and law. IoT also will most likely completely different consequences in several economies and regions, delivery a various set of opportunities and challenges worldwide.

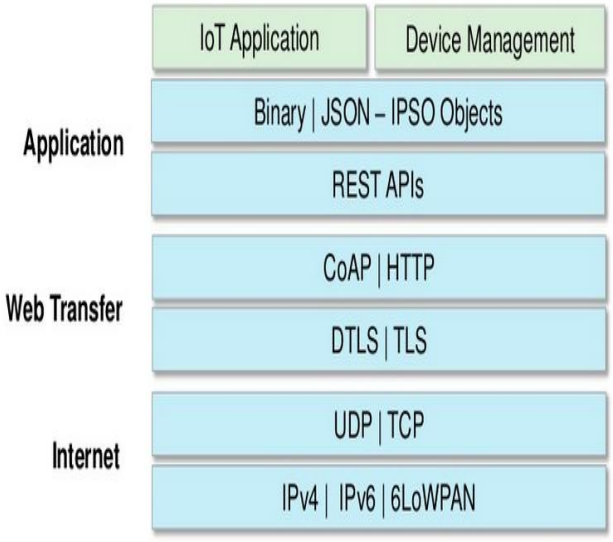

Fig. 1 IoT protocol structure [18]

2. IOT PROTOCOL

In this section discuss some important IoT protocols which is important as per our proposed protocol–

IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. [18]

6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. It is an adaption layer for IPv6 over IEEE802.15.4 links. This protocol operates only in the 2.4 GHz frequency range with 250 kbps transfer rate. [3]

UDP User Datagram Protocol A simple OSI transport layer protocol for client/server network applications based on Internet Protocol (IP). UDP is the main alternative to TCP and one of the oldest network protocols in existence, introduced in 1980. UDP is often used in applications specially tuned for real-time performance.

MQTT (Message Queuing Telemetry Transport)
"The MQTT protocol enables a publish/subscribe messaging model in an extremely lightweight way. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium." **Additional resources [10]**

MQTT-SN (MQTT for Sensor Networks) - An open and lightweight publish/subscribe protocol designed specifically for machine-to-machine and mobile applications. **Mosquitto**: An Open Source MQTT v3.1 Broker IBM Message Sight [11]

CoAP (Constrained Application Protocol)
CoAP is an application layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. The CoRE group has proposed the following features for CoAP: RESTful protocol design minimizing the complexity of mapping with HTTP, Low header overhead and parsing complexity, URI and content-type support, Support for the discovery of resources provided by known CoAP services. [11]

3. PROPOSED METHOD

The proposed method is design to two way authentication based security enhancement for Internet of things (IoT) devices in IPV6 protocol. The proposed improved transmission control protocol (ITCP). Proposals on IoT standardization on protocol and semantic interoperability, security, privacy and trust management issues.

First Step - In the first step of proposed system design in the physical layer. In the physical layer contain IoT devices. There are different IoT and different IEEE standard. For IoT devices standard is IEEE 802.15.4 (MAC) and IEEE 802.15.4 [2.4] GHZ DSSS standard devices are used in this layer. Most of the IoT devices are wireless devices. Some of them based Ethernet connection. In the proposed IoT model is based on both type of IEEE standard that is also shown in fig. 4.3.

IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs). It is maintained by the IEEE 802.15 working group. It is the basis for the ZigBee, ISA100.11a, Wireless HART, and MiWi specifications, each of which further extends the standard by developing the upper layers which are not defined in IEEE 802.15.4. Alternatively, it can be used with 6LoWPAN and standard Internet protocols to build a wireless embedded Internet. **Wi-Fi , WiMax etc.**

Second Step – After the discussion of physical layer and media layer. Next layer is network layer. In the network layer basically focused addressing. There are two different type of addressing IPV4 and IPV6. In first part of the proposed algorithm is used to analyze the problems with the IPV4 protocol based network. In the proposed work analyzed the different type of addressing mode IPV4 and IPV6. For the proposed work is based on the IPV6 based two way authentication system. There are different type of standards are available for the IOT based devise communication.

After the analysis of IPv4 and IPv6 , IPv6 is better for IoT devices in terms of security, Power and number of devices.

Security – IPv6 is more secure is compare to IPv4. Because in the IPv6 contain a 128 bit address in which both address are add physical address of devices that is MAC address and logical address that is IP address. That why provide better security as compare to IPv4 protocol.

Power – IPv6 protocol provide 6LowPAN that is consume low energy as compare to other protocol.

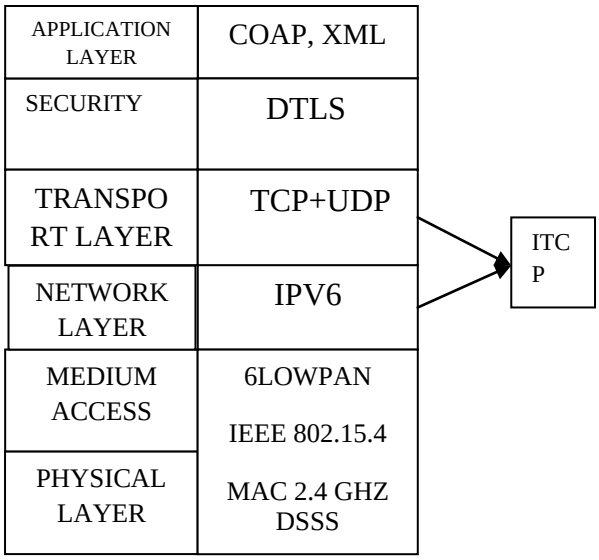

Fig 2 shows the architecture of proposed ITCP method

Third Step –
Transport – In the proposed work use a combination of TCP / UDP combination. In the previous work most of the researcher used UDP protocol for communication between nodes, but in proposed protocol is combination of TCP and UDP protocol.

ITCP – proposed protocol is higher reliable and connection oriented as compare to the UDP protocol

Fourth Step – Apply DTLS algorithm for security purpose, that is provide encryption of the data. The proposed improved transmission control protocol (ITCP) based structure is shown in below figure 2.

4. SIMULATION AND RESULT

The proposed method is simulated on Java Net beans 8.2 that is known as java simulation. Java is important in the field of IoT protocol development. For the comparison of proposed with different previous methods, calculate the different

resultant parameters like throughput, computational time, transmission time, packet delivery ratio (PDR) and packet loss (P.L).

This work, Java based NetBeans IDE 8.2 software version 8.2 and Mysql server is used due to its open source simplicity and free availability. Below figure shows that simulation environment of java and next figure shows the connection of different IoT nodes.

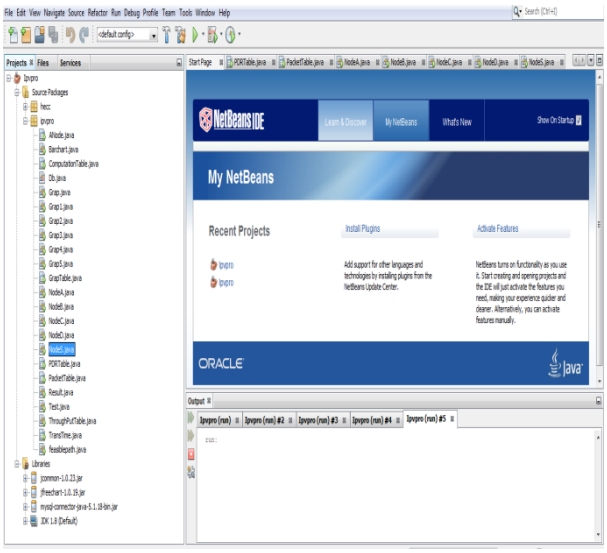

Fig. 3 Shows the Simulation Window of Java based Net beans

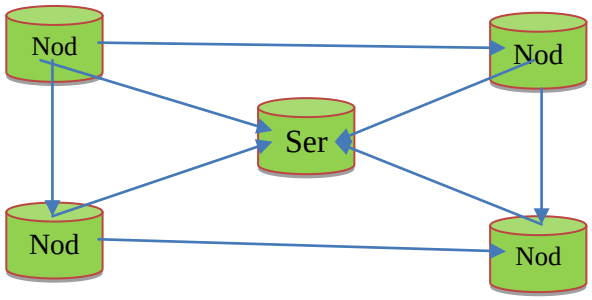

Fig. 4– Shows network structure of proposed work

All these nodes are created in the java script and programmed as like that each node connected with each other via IPv6, after that connected each node via server. For comparison the performance of proposed protocol with other protocols transmission control protocol (TCP), UDP and ITCP.

The main parameters are calculating the performance of network parameters are computation time, throughput, and packet loss are the major player of network performance parameters. All these parameters are ITCP protocol and compare with TCP and UDP protocol finally compare all these results with different previous method at last shown in figure.

Transmission time (TT)

The transmission time of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the length of the string representing the input. All these result are calculate on different data size. Initial perform on small data size after that take bigger data size. 100bits data files start starting data size used up to 1024 bits.

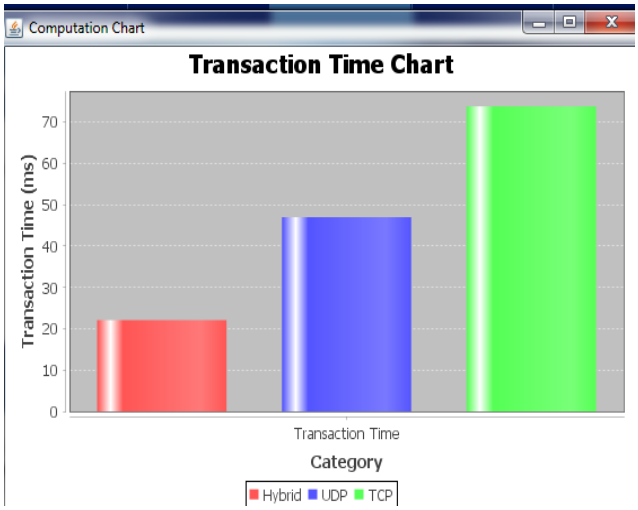

Fig 4 Shows Transaction time in mile seconds (ms)

In the above figure 4 shows the transaction time of proposed method as well as TCP and UDP methods. In the above figure x axis shows the different method and Y axis shows the transaction time in mille second (m.s.). As we clearly see that the transaction time proposed hybrid method is low as compare to other methods.

Table 1 Transaction Time (TT)

Method	Times
TCP	73.85ms
UDP	47ms
Hybrid	22.0825ms

In the above table 1 transaction time shown in numerical values of proposed method and other methods. Transaction time in mille second. After the discussion of transaction time now discuss the throughput of the proposed method.

Throughput

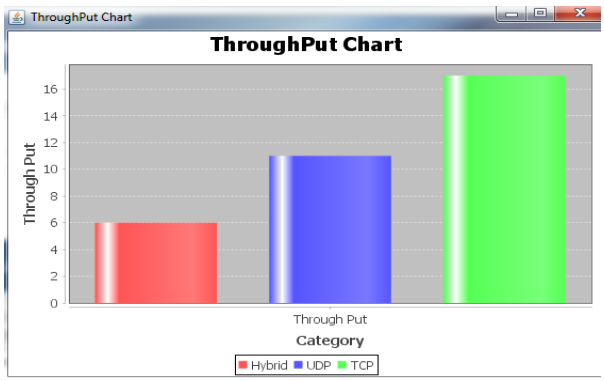

Fig 5 Shows Throughput of method [14]

In the above figure 5. shows the throughput of proposed method as well as TCP and UDP methods. In the above figure x axis shows the different method and Y axis shows the Throughput value which is measured in bit per second. In a single line throughput means number of data packets send per unit time. As we clearly see that the Throughput proposed hybrid method is low as compare to other methods.

Table 2 Throughput

Method	Throughput (bit/second)
TCP	17 b/s
UDP	11 b/s
Hybrid	6 b/s

In the above table 2 Throughput shown in numerical values of proposed method and other methods. Throughput in bites/second. After the discussion of Throughput now discuss the computational time of the proposed method.

Packet Loss (P.L.) [14]

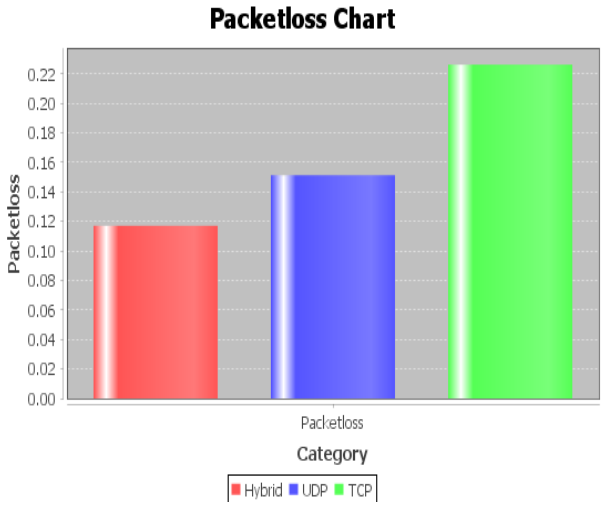

Fig. 6 Shows Packet Loss (PL) method

In the above figure 6 shows the packet loss (PL) of proposed method as well as TCP and UDP methods. In the above figure x axis shows the different method and Y axis shows the Packet loss (PL) which is measured in second. In a single line loss is the failure of one or more transmitted packets to arrive at their destination. As we clearly see that the Packet loss proposed hybrid method is low as compare to other methods.

Comparison

With different previous methods there are given the network has a consistent rate of packet loss, the experienced packet loss of CoAP [11] and custom UDP will take to a level very close to the system rate. On the other hand, both TCP-based protocols MQTT used and last one hybrid that ITCP. ITCP show lower packet loss has compare to different previous protocols UDP CoAP [11], MQTT and proposed ITCP. ITCP shows low packet loss because that is made by combination of TCP and UDP, and perform better as compare to other protocols.

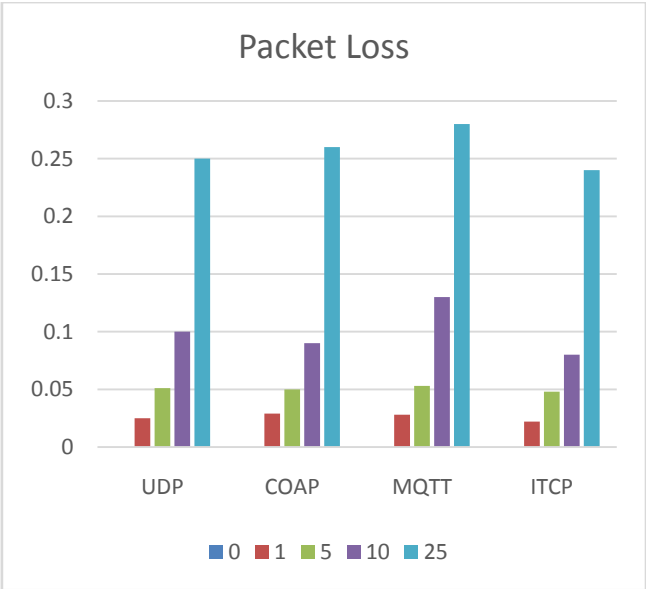

Fig.7 Comparison with Packet loss different protocols

Table 3 Comparison with different protocol

	UDP	COAP	MQTT	ITCP
0	0	0	0	0
1	0.025	0.029	0.028	0.022
5	0.051	0.05	0.053	0.048
10	0.1	0.09	0.13	0.08
25	0.25	0.26	0.28	0.24

5. CONCLUSION

This work, proposed a network layer protocol IoT protocol that improved transmission control protocol (ITCP) protocol. ITCP shows better result as compare to other methods on different result parameters. Also analysis to identify who to improve the quality of IoT that increase the performance of proposed method. We had simulated our proposed solution in the presence of a different node scenarios and traffic. According to the results of the simulation, our technique shows superior performance as PDR and the flow increases however, the packet loss also decreases. In the scenario analysed, it is found that the proposed ITCP has a higher performance then different network layer IoT protocol. The modified protocol is suitable for detection and prevention of attack because having authentication. It improves the delivery ratio of packets under lower B.W., with minimal decrease in throughput and an acceptable increase in performance of overall system.

6. ACKNOWLEDGMENTS

Our thanks to the Ultra-Light technology.

7. REFERENCES

[1] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers, “Twenty security considerations for cloud-supported Internet of Things”, Internet Of Things Journal, IEEE 2015.

[2] Flauzac Olivier, Gonzalez Carlos, Nolot Florent, “New Security Architecture for IoT Network”, International Workshop on Big Data and Data Mining Challenges on

IoT and Pervasive Systems (BigD2M 2015), s. Published by Elsevier, Science Direct, Procardia Computer Science 52 (2015)

[3] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE communications surveys & tutorials July 2015.

[4] Ricardo Neisse, Igor Nai Fovino, Gianmarco Baldini, Vera Stavroulakiy, Panagiotis Vlacheasy and Raffaele Giaffreda "Sec Kit: A Model-based Security Toolkit for the Internet of Things". Computers & Security · September 2014.

[5] John A. Stankovic, "Research Directions for the Internet of Things", National Science Foundation under grants CNS-1239483, CNS-1017363, and CNS-1319302. Copyright (c) 2014 IEEE

[6] Design and Implementation of a Simple User Interface of a Smartphone for the Elderly 2014 IEEE 3rd global conferences on consumer electronics(GCCE)

[7] Securing the IP-based internet of things with HIP and DTLS, April 2013

[8] Research Directions for the Internet of Things 2014 IEEE

[9] Pranay Yadav, "Color Image Noise Removal by Modified Adaptive Threshold Median Filter for RVIN" , Electronic Design, Computer Networks & Automated Verification (EDCAV), 2015 pp - 175 - 180, 29-30 ,

[10] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig, Georg Carle, "DTLS based Security and Two-Way Authentication for the Internet of Things", Elsevier Journal of AdHoc Networks in May 2013.

[11] Z. Shelby, K. Hartke, C. Bormann, B. Frank, Constrained Application Protocol (CoAP), IETF draft, RFC Editor (March 2013).

[12] Slimfit — A HIP DEX compression layer for the IP-based Internet of Things , OCTOBER 2013

[13] Convergence of MANET and WSN in IoT urban scenarios IEEE SENSORS JOURNAL · OCTOBER 2013.

[14] Yadav P., Sharma S., Tiwari P., Dey N., Ashour A.S., Nguyen G.N. "A Modified Hybrid Structure for Next Generation Super High Speed Communication using TDLTE and Wi-Max" for publication in *Studies in Big Data, Springer* **2017.** https://link.springer.com/chapter/10.1007/978-3-319-60435-0_21#citeas.

[15] Early infrastructure of an Internet of Things in Spaces for Learning Eighth IEEE International Conference on Advanced Learning Technologies 2012.

[16] S. Raza, T. Voigt, V. Jutvik, and Lightweight IKEv2: A Key Management Solution for both the Compressed IPsec and the IEEE 802.15.4 Security, in: Proceedings of the IETF Workshop on Smart Object Security, 2012.

[17] Pranay Yadav and Parool Singh2, "Color Impulse Noise Removal by Modified Alpha Trimmed Median Mean Filter for FVIN", IEEE International Conference on Computational Intelligence and Computing (IEEE-ICCIC), pp: 1 – 8, 10.1109/ICCIC.2014.7238369, Dec – 2014.

[18] Tobias Heer, Oscar Garcia-Morchony, Rene Hummen, Sye Loong Keohy, Sandeep S. Kumary, and Klaus Wehrle, "Security Challenges in the IP-based Internet of Things", Springer Journal on Wireless Personal Communications, December 2011, Volume 61, Issue 3, pp 527-542.

[19] Embedded security for Internet of Things APRIL 2011 DOI: 10.1109/NCETACS.2011.5751382 · Source: IEEE Xplore

[20] Sharma, S. and Yadav, P, "Removal of Fixed Valued Impulse Noise by Improved Trimmed Mean Median Filter" IEEE International Conference on Computational Intelligence and Computing **(**IEEE-ICCIC)pp: 1 - 8, DOI: 10.1109/ICCIC.2014.7238368,.

[21] S. Dawson-Haggerty, A. Tavakoli, D. Culler, Hydro: A Hybrid Routing Protocol for Low-Power and Lossy Networks, in: Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Smart Grid Comm, 2010, pp. 268-273

[22] W. Hu, H. Tan, P. Corke, W. C. Shih, S. Jha, Toward Trusted Wireless Sensor Networks, ACM Transactions on Sensor Networks 7 (2010) 5:1-5:25.

[23] W. Jung, S. Hong, M. Ha, Y.-J. Kim, D. Kim, SSL-Based Lightweight Security of IP-Based Wireless Sensor Networks, International Conference on Advanced Information Networking and Applications Workshops (2009) 1112-1117.

[24] D. Raymond, S. Midki_, Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses, Pervasive Computing 7 (1) (2008).

[25] Luk, G. Mezzour, A. Perrig, V. Gligor, MiniSec: A Secure Sensor Network Communication Architecture, in: Proceedings of the 6th International Conference on Information Processing in Sensor Networks, IPSN, 2007, pp. 479-488

[26] M. Wurm, Y. Zhu, M. Millard, S. Fung, N. Gura, H. Eberle, S. C. Shantz, Sizzle: A Standards-based End-to-End Security Architecture for the Embedded Internet, Pervasive Mob. Comput. 1 (2005) 425-445.

[27] H. Chan, A. Perrig, D. Song, Random Key Predistribution Schemes for Sensor Networks, in: Proceedings of Symposium on Security and Privacy, 2003,