International Journal of Engineering & Technology, 7 (4.28) (2018) 595 -598

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Effectual Algorithm for Avoidance of Version Number Attacks in Internet of Things (IoT)

Dr. Esraa Saleh Alomari

Computer science, computer science & IT collage, Wasit University

Abstract

Internet of Things (IoT) is one of the emerging domains in the wireless communication and technologies whereby the sensor based devices interact with each other using radio frequencies. The enormous work is going on in this segment to enrich the security still there is huge scope of research. In IoT, the implementations of Vehicular Adhoc Networks (VANET), Internet of Vehicles (IoV), Smart Offices, Smart Cities are quite prominent which are addressed in this research work. With the use of soft computing approaches, the implementation of higher degree of security can be done. "In this research manuscript, the approach to integrate the dynamic key exchange with the Elephant Herd Optimization (EHO) is presented to achieve the higher degree of energy optimization and overall lifetime of the network communication. The key concept of the cluster head shuffling using EHO and inner modules of key exchange are simulated in Contiki-Cooja that is open source simulator for advance wireless networks". But the version number attacks can destroy the overall scenario and the performance in which the exploitation of multiple resources can be done. In this research work, the approach to defeat and push back the version number attacks in RPL using dynamic security is implemented and evaluated on multiple parameters.

Keywords: *Advance Wireless Networks, Energy Aware Wireless Networks, Power and Energy Optimized Wireless Systems*

1. Introduction

Kevin Ashton (1999) presented the paradigm of Internet of Things (IoT) in which the connectivity of multiple objects was underlined using wireless technologies in integration of the radio frequency. The technologies associated with IoT include smart gadgets and assorted sensor based devices which communicate with each other using wireless signals. The reports from Forbes depicts that the cumulative market share of IoT will reach 267 billion dollars with the touch of year 2020 while the reports from Gartner, a prominent research agency depicts that around 9 billion objects will be connected with each other with the investment span of 273 billion dollars in the existing year of 2017.

2. Routing Protocol over Low Power and Lossy Networks (RPL) and Version Number Attacks

RPL is the key protocol that works with IPV6 to implement the communication and secured transmission in the environment of Internet of Things (IoT). Most of the implementations of IoT integrate RPL that is the focused routing protocol over low power and lossy networks. As per the analytics and documentation from Internet Engineering Task Force (IETF), RPL refers to the routing protocol specifically developed for low power as well as lossy networks commonly referred to as LLN. The Low Power and Lossy Networks (LLNs) signifies the unique and effectual class in the wireless network where the constrained perspectives of routers and related interconnect objects exist. The routers of LLN classically function with the limitations of memory, power, battery, energy and related dimensions.

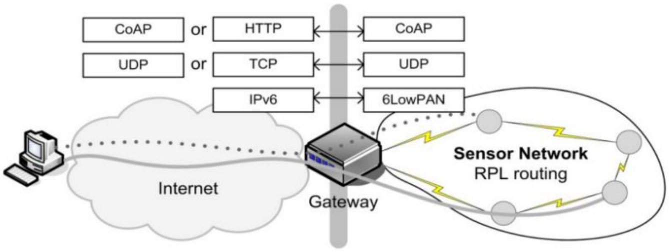
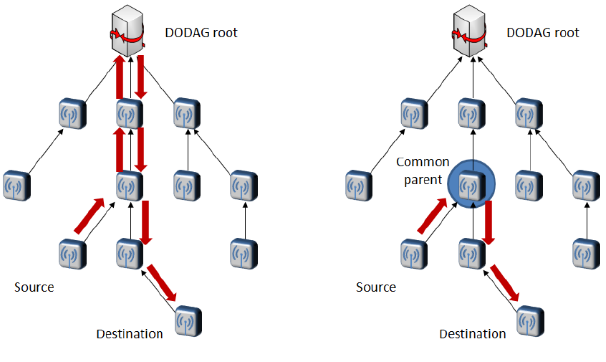


Figure 1. Low Power and Lossy Network Environment with RPL Routing



P2P traffic in non-storing mode

P2P traffic in storing mode

Figure 2. Flow of the Packets and Nodes in RPL Network

The packets flow in lossy networks with RPL is depicted in the figure in which the node listens to get the DODAG information object (DIO). Here, DODAG refers to Destination Oriented Directed Acyclic Graph. The new node in IoT network analyzes the

DODAG signal and responds. In case there is no signal or message from DIO, the node simply broadcast the DIS that signifies DODAG Information Solicitation to direct the other surrounding nodes to transmit the DIO message. There are two modes in the operation which includes Fully Stateful (Storing) or Fully Source Routed (Non-Storing) mode. The storing case includes the approach in which the packets move and directed to the downward to reach the destination using the common ancestor related to the source. In non-storing mode, the packet moves and traverses all the way and paths towards DODAG root rather than directly moving down to the destination.

3. Literature Review

"Q. Jing et al. (2014) worked on Radio Frequency Based Objects and Security. This work underlines the issues and problems associated with security and vulnerability and the approaches by which the overall IoT scenario can be made secured and performance aware".

Z. Yan (2014) underlines the work on Trust Architecture and Overall Security Enhancement. The security perspectives of IoT are presented in this work with the integration of Privacy-Preserved Data Mining (PPDM), Privacy-Preserved Intrusion Detection (PPID), Privacy-Preserved Database Query (PPDQ) and Privacy-Preserved Scientific Computations (PPSC) as the key approaches to escalate the overall scenario of security and integrity of IoT Network.

D. Lake et al. (2014) presented IoT in Healthcare. "The work includes and focuses on secured architecture framework with the multilayered approach having key elements of connection, collection, correlation, calculation, conclusion and collaboration".

"Y. Ning (2014) evaluated the Perception Layer Security. The proposed approach Attribute-based Access Control (ABAC) performs the effective implementation on the parameters of security and resource optimization with higher degree of integrity and overall performance".

"M. Turkanovic (2014) worked on Hybrid Authentication. The approach of hybrid authentication is presented in this work with the multiple panels and dashboard for secured login and identification of the attempt with the evaluation of the type of attempt in the IoT network".

S. Sicari (2015) worked on Security and Privacy Aware Architecture. The work includes the proposed schemes and protocols to make them secured and integrity aware for any type of assault.

J. Granjal (2015) implements and focused on IoT Architecture. In addition, the work in having key focus on the protection and security formulations associated with each protocol.

"K. T. Nguyen (2015) focused on IPv6 Security. Moreover, the key exchange mechanisms and their relative efficiency along with the security is underlined in this research manuscript.

M. Vucinic et al. (2015) worked on Object Security Architecture for the Internet of Things (OSCAR) to protect against the replay attacks and security of data channels in the Internet of Things".

"W. Trappe (2015) presented the work on Resource Optimization using Multi-layered Architecture escalation of security factor with its impact on the energy and other perspectives so that the integrity and consistency can be maintained in the overall IoT scenario".

"F. Li et al. (2016) focused on Multi-Key Security. Heterogeneous ring based encryption technique to achieve the confidentiality, security, overall integrity and related non-repudiation factors in the network".

"S. R. Moosavi (2016) evaluated security with the multidimensional mobility. The resource optimization factors in this scheme are very effective and achieving the performance and speed to 97%".

"K. A. Rehiman (2016) underlined the work of Secured Key Based Approach. The novel approach used in this work is based on the zero knowledge protocol as well as dynamic hashing for achieving the secured authentication in IoT environment".

"D. Airehrour (2016) worked on Secured IoT Routing. As per the authors in this paper, there is need to devise and work on the multilayered approaches for security and integrity in the smart objects or smart mobile devices in the Internet of Things so that overall communication can be made secured and integrity aware".

"E. Bertino (2016) focused on Trust Management. The research manuscript presented the key challenges associated with the data security and integrity with the efficient as well as scalable protocols for security and encryption".

"M. Usman et al. (2017) implements SIT Encryption in five iterations or passes which are very less as compared to the traditional approach and that’s why it is less complex".

"M. B. Mollah et al. (2017) focused on the key area of IoT with Cloud Technologies. The scenario taken here is the Cloud assisted IoT by which the smart objects are able to communicate effectively"

P. P. Jayaraman et al. (2017) implements Multilayered Architecture for Security. The proposed work is done using OpenIoT platform for the implementation and multiple cloud based IoT networks are simulated in this research work.

"C. Schmitt et al. (2017) presented two way solutions for the authentication and overall security in the Low Power Wireless Networks. This work is based on the focus towards Datagram Transport Layer Security (DTLS) by which the overall security and resource optimization can be achieved to a higher extent".

"S. Prabhakar (2017) evaluated and associated IoT and Cloud Environment. The work includes the focus to vulnerabilities and different susceptibility factors in network and the usage of different mechanisms to avoid these assaults".

4. Elephant Herd Optimization with Dynamic Key Exchange

```
Begin
        Initialize nodes and Activation as Elephant Object
Initialize source and destination nodes with Random Energy Parameters and Threshold
FOR $i = 0\ to\ Number\ of\ Nodes\ (n)$ DO
$Cluster\ Head\ Formation\ CHF_i$ ← Dynamic Selection of the Cluster Head based on the Fitness Score in Elephant Herd Optimization (EHO)
                IF (RFID Sensor fitness score maintain) THEN
                        $Transmit\ common\ identifier$
                        Integration of Nature Inspired Approach Module
Dynamic Key Exchange for Higher Degree of Security and Lifetime
                ELSE
                        Re-Evaluate the Fitness Score
Allocate the CHF and Re-Selection Criteria Initiates
                END IF
END FOR
FOR $i = 0\ to\ Number\ of\ Nodes\ (n)$ DO
                IF (CHF transmission and leading successful) THEN
                        $Forward\ RREQ \rightarrow destination\ node$
                        Integration of Nature Inspired Approach Module on Threshold
                        Acceptance of Results and Logs
                ELSE
                        $Forward\ RREQ \rightarrow\ CH_i$
                        $CH_i\ \rightarrow BS_i\ BS_i\ \rightarrow CH_i$
                        $CH_i \rightarrow destination\ node$
                        Threshold Evaluation and Fitness of Results
                END IF
```

```
            END FOR
      END FOR
END
```

"The key points of proposed approach with EHO includes the perspectives that higher level of optimization of energy using Dynamic Cluster Head Selection (DCHS) and Shuffling for unbiased and performance aware approach". "There is integration of formation of dynamic topology so that the consistency can be checked and evaluated along with the dynamic Hash Key based Transmission to avoid Energy Consuming Assaults and achieving power and energy aware transmission for escalated lifetime. The assignment of weights and other parameters of sensor nodes".

5. Implementation and Results

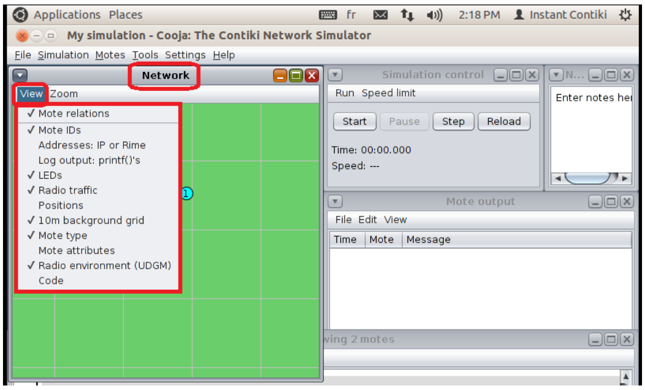


Figure 3. Implementation Scenario of IoT in Cooja Simulator

Figure 3 depicts the implementation scenario of Internet of Things (IoT) in Cooja simulator under Contiki Platform. Contiki is one of the key platforms for implementation of IoT scenarios along with the integration of real sensors so that the live data can be fetched. In actual facts, Contiki platform is a flavor of Ubuntu Linux that is one of the powerful operating system for different types of applications including Wireless Simulations, Cloud Platforms, Big Data and many others.

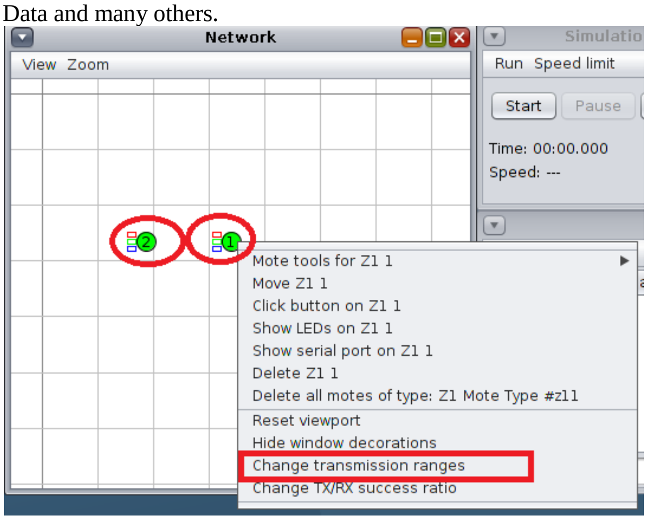
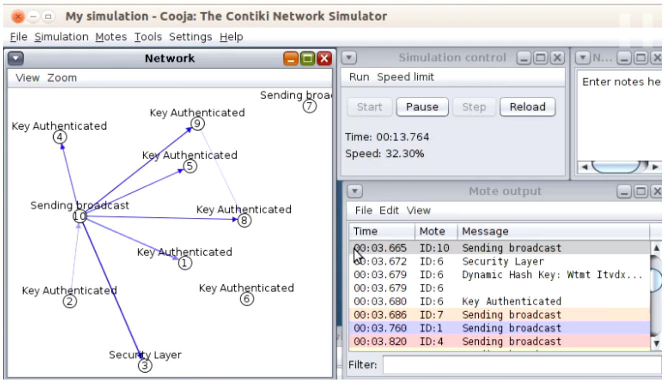


Figure 4. Setup of the Wireless Radio Properties in Cooja Simulation

Figure 4 presents the setup of transmission ranges which are placed with the sensor nodes to have the desired behavior of the RFID sensor nodes. Using this, the transmission ranges can be set to different levels.

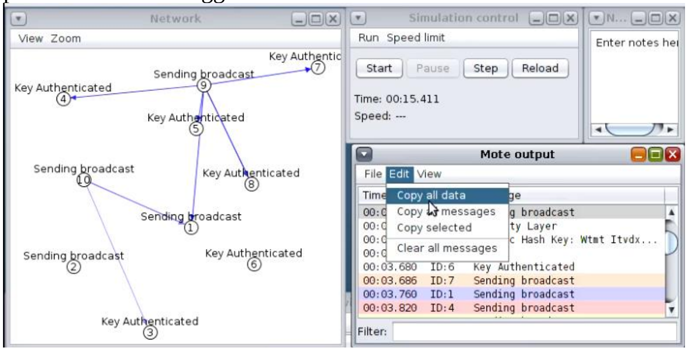


Time: 00:13.764
Speed: 32.30%

```
Time       Mote   Message
00:03.665  ID:10  Sending broadcast
00:03.672  ID:6   Security Layer
00:03.679  ID:6   Dynamic Hash Key: Wtmt Itvdx...
00:03.679  ID:6
00:03.680  ID:6   Key Authenticated
00:03.686  ID:7   Sending broadcast
00:03.760  ID:1   Sending broadcast
00:03.820  ID:4   Sending broadcast
```

Figure 5. Elephant Herd Optimization (EHO) for Dynamic Security and Energy Optimization in Cooja

Figure 5 and Figure 6 depicts the simulation of EHO in the network simulation with the process of key authentication and logging of the status so that the packets loss, temperature, energy and other parameters can be logged.



Time: 00:15.411
Speed: ---

```
Time                    ge
00:0                    g broadcast
00:0                    ty Layer
00:0                    c Hash Key: Wtmt Itvdx...
00:0
00:03.680  ID:6   Key Authenticated
00:03.686  ID:7   Sending broadcast
00:03.760  ID:1   Sending broadcast
00:03.820  ID:4   Sending broadcast
```

Figure 6. Dynamic Fetching of the Logs and Message from Simulation

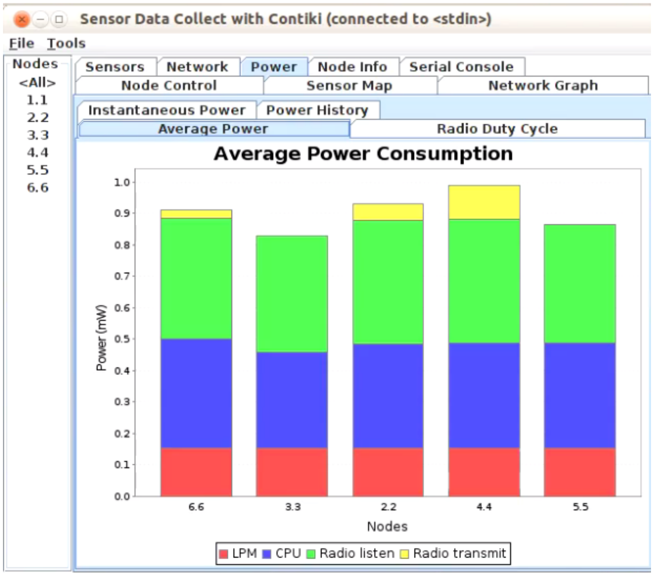


Figure 7. Evaluation of Power Consumption from Simulation and Execution Scenario

There are multiple parameters which are evaluated after execution and simulation run. These parameters include Radio Listen, LPM and Radio Transmit which are evaluated from Cooja simulation in Contiki platform. The output is consistent in terms of multiple parameters and no biasing or mismatch is found. The results found are integrity aware as per the output from Cooja simulation on multiple sensor nodes.

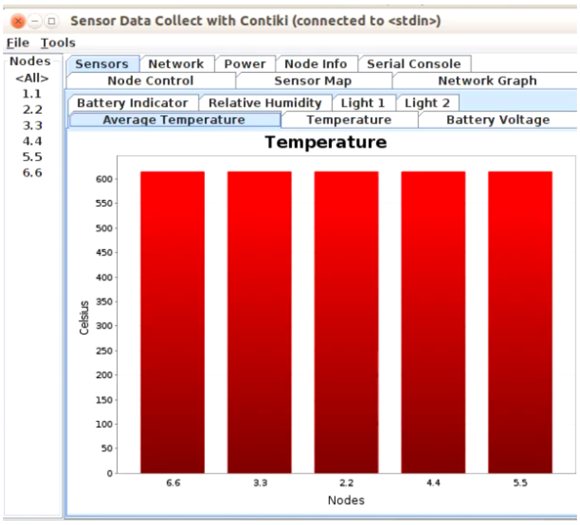


Figure 8. Temperature Evaluations in Celsius at the Motes

There is consistency and integrity in the temperature parameter as in the results from Figure. The minimum and almost equal temperature decay is reported from the Cooja simulation on integration of multiple nodes in the IoT environment.

6. Conclusion

"The use of metaheuristic or nature inspired approaches is always in research to achieve the higher degree of accuracy. This work is having the key focus on the use of Elephant Herd Optimization. The proposed approach is having higher degree of lifetime, accuracy and overall optimization factors". Nature Inspired Approaches are widely used for solving optimization problems from a long time and that’s why this dimension is adopted to be implemented in the wireless networks."The proposed approach is evaluated on multiple parameters including energy optimized, accuracy, turnaround time and overall performance of the network. The wireless nodes with degree of energy and lifetime are given occasion to be cluster head so that overall performance and lifetime of the clustered environment can be escalated".

References

[1] Zanella A, N. Bui, A. Castellani, L. Vangelista and L, Zorzi. “Internet of things for smart cities” IEEE Internet of Things Journal. pp. 22-32., 2014

[2] Zhang, K., Liang, X., Lu, R., & Shen, X. “Sybil attacks and their defenses in the internet of things.” IEEE Internet of Things Journal, 1(5), 372-383, 2014

[3] Farooq MU, Waseem M, Khairi A, Mazhar S. “A critical analysis on the security concerns of internet of things (IoT).” International Journal of Computer Applications. pp. 1-7, 2015

[4] Stankovic JA. “Research directions for the internet of things”. IEEE Internet of Things Journal. pp 3-9, 2014

[5] O. Said, M. Masud., “Towards internet of things: Survey and future vision”. International Journal of Computer Networks. pp.1-7, 2015

[6] Perera C, Zaslavsky A, Christen P, Georgakopoulos D. “Context aware computing for the internet of things: A survey”, IEEE Communications Surveys & Tutorials., 414-454, 2014.

[7] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[8] L. Chen, Z. Yan, W. Zhang, and R. Kantola, “TruSMS: A trustworthy SMS spam control system based on trust management,” Future Generation Computer Systems, vol. 49, no. October, pp. 77–93, 2015.

[9] D. Lake, R. Milito, M. Morrow, and R. Vargheese, “Internet of Things: Architectural Framework for eHealth Security,” Journal of ICT, vol. 1, no. 3, pp. 301–328, 2014.

[10] N. Ye, Y. Zhu, R. C. Wang, R. Malekian, and Q. M. Lin, “An efficient authentication and access control scheme for perception layer of internet of things,” Appl. Math. Inf. Sci., vol. 8, no. 4, pp. 1617–1624, 2014.

[11] M. Turkanović, B. Brumen, and M. Hölbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion,” Ad Hoc Networks, vol. 20, no. April, pp. 96–112, 2014.

[12] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.

[13] J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the internet of things: A survey of existing protocols and open research issues,” IEEE Commun. Surv. Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.

[14] K. T. Nguyen, M. Laurent, and N. Oualha, “Survey on secure communication protocols for the Internet of Things,” Ad Hoc Networks, vol. 32, no. February, pp. 17–31, 2015.

[15] M. Vucinic, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, “OSCAR: Object Security Architecture for the Internet of Things,” Science Direct Ad Hoc Networks, pp. 3-16, 2014.

[16] W. Trappe, R. Howard, and R. S. Moore, “Low-energy security: Limits and opportunities in the internet of things,” IEEE Security and Privacy, vol. 13, no. 1, pp. 14–21, 2015.

[17] F. Li, Z. Zheng, and C. Jin, “Secure and efficient data transmission in the Internet of Things,” Telecommunication Systems, vol. 62, no. 1, pp. 111–122, 2016.

[18] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, “End-to-end security scheme for mobility enabled healthcare Internet of Things,” Futur. Gener. Comput. Syst., vol. 64, no. May, pp. 108–124, 2016.

[19] K. A. Rafidha Rehiman and S. Veni, “A secure authentication infrastructure for IoT enabled smart mobile devices - an initial prototype,” Indian J. Sci. Technol., vol. 9, no. 9, pp. 1-6 2016.

[20] D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for internet of things: A survey,” Journal of Network and Computer Applications., vol. 66, pp. 198–213, 2016.

[21] E. Bertino, “Data Security and Privacy in the IoT,” Proc. 19th Int. Conf. Extending Database Technol., Open Proceedings, pp. 1–3, 2016.

[22] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, “SIT : A Lightweight Encryption Algorithm for Secure Internet of Things,” International Journal of Advanced Computer Science and Applications, vol. 8, no. 1, pp. 1–10, 2017.

[23] M. B. Mollah, A. K. Azad, and A. Vasilakos, “Secure data sharing and searching at the edge of cloud-assisted internet of things,” IEEE Cloud Computing, vol. 4, no. 1, pp. 34–42, 2017.

[24] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, “Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation,” Future Generation Computer Systems, pp. 1–10, 2017.

[25] Schmitt, M. Noack, W. Hu, T. Kothmayr, and B. Stiller, “Two-way Authentication for the Internet-of-Things,” Securing Internet Things through Progress. IGI Global Journals, pp. 27-56, 2017.

[26] S. Prabhakar. International Journal of Research in Computer Applications and Robotics, vol. 3, no. 6, pp. 93-101, 2017.