Authentication and Encryption for a Robotic Ad Hoc Network using Identity-Based Cryptography

Jonay Suárez-Armas, Alexandra Rivero-García, Pino Caballero-Gil and Cándido Caballero-Gil

Department of Computer Engineering and Systems

University of La Laguna

Tenerife, Spain

{jsuarear,ariverog,pcaballe,ccabgil}@ull.edu.es

Abstract—In some situations the communications of a place can be affected, totally lost, or not even exist. In these cases, the MANETs play an important role, allowing to establish a communications point using the different nodes of the network to reach the destination using decentralized communications. This paper proposes the implementation of a Robotic MANET, a decentralized network using robots as its nodes, which allows to move the network nodes to the desired location remotely. For this, each robot has as a core a Raspberry Pi with the capabilities to perform audio and video streaming, remote control of robots, tracking of objects, and deployment of wireless networks. To protect the network, different security mechanisms are used that allow secure authentication on the network by different nodes and encryption of information transmitted between them. All communications are protected through Identity-Based Cryptography, specifically with an Identity-Based Signcryption scheme.

Index Terms—Network, MANET, Robotic, Authentication, Encryption

I. INTRODUCTION

In a world in which technology has been incorporated, both in business and homes, communications have become essential. Due to the centralization of information and storage of data in the cloud, a failure in communications (especially in the business environment) can cause chaos. If this happens in a population nucleus instead of an enterprise, the consequences can be much more serious, especially if it is due to a natural disaster or some kind of catastrophe.

When there is a communications outage situation, it is about finding a solution, establishing a temporary communications point that allows, at least, to have a connection point that allows basic communications to maintain control of the situation.

Unlike centralized communications, decentralized or distributed communications enable direct communication between devices in a network. This means that in this type of communications it is not necessary to have a central device so that the different devices in the network can communicate. Between these two topologies, there is also an intermediate case called hybrid (See Fig. 1).

In order to establish a communications point in a place where communications have broken down or a temporary communication point is desired, this paper proposes a MANET (Mobile Ad Hoc Network) based on the use of robots that could adopt the acronym R-MANET (Robotic Mobile Ad Hoc

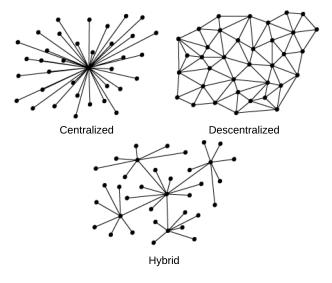


Fig. 1. Network topologies.

Network) or directly RANET (Robotic Ad Hoc Network). The robots will be in charge of forming a multi-hop [1] network to finally provide a communications point to the place where the network final nodes (robots) are established.

Robotics has increasingly gone into homes, to the point that we have kitchen robots [2], or robots that clean the floor [3] for us. The latter, vacuum cleaners have several advantages such as the possibility of returning automatically to the battery charging station when necessary, so they are being used for other tasks that are not related to cleaning. The proposal therefore uses vacuum robots as network nodes.

In this work, the security of the proposed system is an essential component. We work in the form of authentication of the different network nodes, verifying that each of them are authorized by the network. In addition, a way of encrypting the data is proposed, so that communications are secure and the information will be protected from the sender to the receiver. An IDentity-Based Signcryption (IDBS) [4] is used for communication confidentiality, authenticity and integrity, both among peers, and between the central station and robots.

The following section discusses a series of works close to the proposal made. Section 3 explains the proposed system in more detail and section 4 also details the components of each robot-based network node. Section 5 shows the security mechanisms used in the proposed system. Finally, a conclusion close the paper.

II. RELATED WORKS

One of the fields in which decentralised communications can be very important is in IoT [5] (Internet of Things). More and more devices are connected, and it may be really interesting that between them they form a Wireless Sensor Network (WSN). Many times, this type of network can be the solution for sending data to the cloud when the device does not have a direct Internet connection, but jumping between devices is able to send the information to one with an Internet connection available. In [6], different Multi-Hop routing protocols for Ad Hoc wireless networks are studied and compared. In this type of network, it is important to measure transmission rates between nodes, so that you can choose the optimal way to send information more quickly and efficiently [7].

In IoT, different works are based on the use of Raspberry Pi for data collection through sensors that form WSAN (Wireless Sensor and Actuator Network), which form a MANET between the different devices for data transmission between them [8]. Another device used in these sensor networks is the Arduino microcontroller, as in [9], which form a network of sensors for temperature monitoring and to help air conditioning systems operate more efficiently.

The increase in computing capacity of smartphones has also made them useful for decentralized networking. Bluetooth is one of the technologies chosen to form MANET networks between mobile devices [10]. These devices are also used to create VANETs that allow the exchange of information between vehicles on the road [11], so that they can share some useful information such as traffic status. The ability to obtain data through built-in sensors means that smartphones can be mounted on a device to move it to one location and obtain data [12], sometimes forming a MANET to deploy several devices at once.

MANET networks are also mounted on drones, such as in [13], where these networks are used to increase the coverage range of the remote control.

The iRobot Roomba robots apart from the tasks for which they have been designed [14], are able to perform other actions thanks to the Open Interface that it has, through which it is possible to send commands. This, in addition to the low cost of these robots, has caused them to be used for different jobs [15]. In [16], the authors have worked on the control of an iRobot robot using an external keyboard and voice commands. In [17], a camera is placed on a Roomba robot to compare the captured video with one previously recorded to detect if there are abandoned objects in the examined area. Moreover, by applying fuzzy logic to these robots [18] it is possible to develop navigation systems that allow them to obtain more optimal routes while are avoiding obstacles in their path.

In a decentralised network, it is very important to take into account its security. Two of the aspects to be studied are the form of authentication in the network and the protection of the data that is sent between the different nodes until reaching the final destination. Some authors propose models for authentication and auto-configuration of nodes in MANET networks [19] and even on preventing impersonation attacks using double authentication factor [20]. Apart from this, [21] studies different cryptographic protocols for use in MANETs at the level of energy consumption, which is important in mobile devices, concluding that the AES standard is the one that produces the best performance among the different algorithms analyzed.

III. PROPOSAL DESCRIPTION

The system proposed in this paper is a MANET in which the different network nodes are robots. The aim is to place the different nodes in the necessary positions to form a network in which a communications point is established at the end point. This communication point will provide the possibility of having a voice and/or data connection in an area that for some reason is out of communication, and where communications with other places are needed. The use of robots as network nodes allows each node to be moved remotely to the desired location, which can be important if it is a dangerous area for people to transport equipment.

To start with the deployment of the robots that will form the network, first you must study the area and calculate the number of nodes needed to extend the network. This calculation is made considering the maximum range of wireless technology used for the connection between the nodes. It should be noted that in general, the theoretical maximum ranges in practice can decrease considerably. The technology chosen to deploy the network is Wi-Fi [22], which has a maximum range of 100 meters. If, for example, we wanted to establish a communications point 500 meters from the starting area, the theory tells us that we would have to form a network with 5 nodes to reach the desired area. To this we must add the base station located at the starting point, from which the signal is transmitted and the network is controlled. The diagram in Fig. 2 shows the general idea of the proposal.

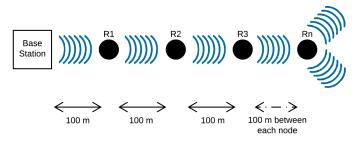


Fig. 2. Network scheme.

The system proposed to deploy a temporary communication point through the use of robots is based on different functionalities: remote control of robots, streaming, object tracking and wireless network deployment.

First of all, there is the remote control of robots. This functionality allows each node of the network to be moved remotely to the point where it has been previously decided. From the base station it is possible to select a robot within the network and send it real-time movement commands.

Secondly, we have audio and video streaming [23]. To be able to move the robots remotely, it is necessary to know where they are at any given moment, so this second functionality is essential. Thanks to streaming, it is possible to visualize the environment in which the robot is located, at the same time that it is remotely controlled from the base station. In addition, audio is included in the streaming in case it would be useful to listen to the sound of the environment in which it is moving. To carry out this functionality, the base station must have a streaming server to which each robot will send the audio and video signal. The RTSP protocol [24] is used to send this signal from the robots to the streaming server, and the RTMP protocol [25] is used for receiving the video from the server to the base station equipment. In both cases, port 1935 is used (See Fig. 3).

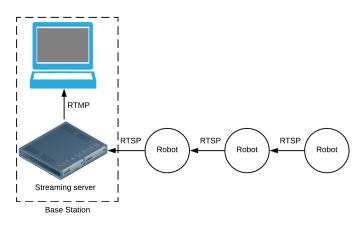


Fig. 3. Streaming scheme.

To perform these two functions, a web application is incorporated in the base station. It shows different blocks, and each one of the blocks refers to a robot, showing in them the video received through streaming together with buttons that allow sending movement orders to each robot.

Third is object tracking [26], which is used for the most interesting part of the proposal. Directing each robot remotely to the desired location can be a tedious task (especially if the number of nodes is too large), so it is proposed that by controlling only one of the robots the rest will be able to follow it autonomously. For this, a master node will be selected and the rest will be slaves of it. Each robot has a QR code on the back that identifies it within the network. Each slave robot has to do image recognition, looking for any QR code in the images captured by your camera. This is when the robot has to check if the detected QR code corresponds with the robot you have programmed to follow. The flowchart of Fig. 4 shows this process.

Once a slave robot has detected the QR code of the robot to be followed, it performs calculations to establish the adequate movement. To do this, a proximity sensor is used, so that if the robot is more than a certain distance away, it has to

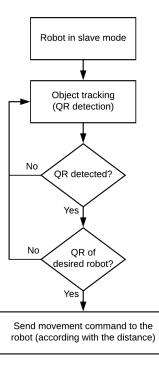


Fig. 4. Flowchart of robot tracking.

start following the predecessor robot. In addition, depending on the area of the image in which the QR of the front node is detected, it will move in a certain direction (See Fig. 5).



Fig. 5. QR detection.

The latest functionality is responsible for deploying a wireless network at each node of the network. Each robot receives the Wi-Fi signal from its predecessor, so that it can have a connection to the base station by jumping between the different nodes in the network. In turn, they need to deploy a new Wi-Fi network so that the next node can connect to it to maintain a connection chain between the base station and the end node.

IV. NODE DESCRIPTION

So far, the proposed system for deploying a RANET has been described, but the technologies and elements available to each network node have not been defined. It has also not been specified what type of robot is used.

Each node is built around an iRobot Roomba [27] vacuum robot, which is connected to a Raspberry Pi, these two forming the core of the node. The Raspberry Pi is connected to the robot to send commands to it and is also responsible for establishing communications with the base station and the other nodes of the network.

As can be seen in the connection diagram of the different elements (See Fig. 6), the Raspberry Pi is the central element of the node (all elements are connected to it thanks to the USB ports that it incorporates, GPIO pins or ports for specific use).

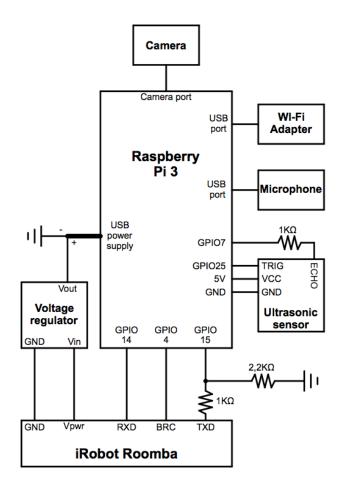


Fig. 6. Node wiring diagram.

First of all there is the camera, which is connected through a specific port that incorporates the Raspberry Pi. Second are the USB ports, which are used to connect a second Wi-Fi adapter and a microphone for audio reception. Thirdly, an ultrasonic sensor is connected to the GPIO pins for detecting obstacles (adding a resistance that adjusts the tension provided on the Raspberry Pi) and the Roomba robot. To connect the robot, a resistive voltage divider [28] is incorporated in the Roomba

transmission pin to reduce the 5V supplied by it to a maximum of 3.3V, which allows the Raspberry Pi reception port.

$$V_{out} = \frac{R_2}{R_1 + R_2} \cdot V_{in}$$

And finally there is the connection of the Raspberry Pi's power supply. Taking advantage of the fact that the Roomba is able to provide power to external devices, the battery is used to avoid having to incorporate an external one, using a voltage regulator that converts the 14.4V that provides the Roomba battery to the 5V that Raspberry Pi needs.

In addition to the Wi-Fi interface that Raspberry Pi incorporates, a second interface has been added through the USB port to extend the network that gets the first interface, so that an interface is used in the usual reception mode, and the second is configured in Ad Hoc mode. For simpler configuration of network interfaces, as well as to allow external devices to connect to wireless networks created by different network nodes, a single class B network [29] will be configured, which allows the connection of 65534 devices (discounting the base station and broadcast address), among which may be network nodes, or end devices. It should be noted that each network node will use 2 IP addresses, as it has two wireless cards; instead, each end device will use a single IP address. IP addressing of devices connected to the network is carried out automatically thanks to the incorporation of a DHCP server in the base station. To do this, a range of addresses is reserved for the network nodes, and all other addresses are assigned automatically.

V. SECURITY

The security of communications is a crucial point of the system. An ID-Based Signcryption scheme (IBSC) is used in order to achieve secure communications. This kind of cryptosystem is a combination of ID-Based Encryption (IBE) and ID-Based Signature (IBS), where all the shared messages are encrypted and signed. This proposed scheme offers the advantage of simplifying management of keys by not having to define a public key infrastructure. A part of this, this scheme has a low computational complexity and it is efficient in terms of memory. In this RANET system, the identification of nodes is a crucial point. Each robot has a QR code on the back that identifies it with a unique ID, this is the public identification used for the IBSC.

First of all, some mathematical tools used is described. Let consider (G, +) and (V, \cdot) be two cyclic groups of the same prime order q. P is a generator of G and there is a bilinear map paring $\hat{e}: G \times G \to V$ satisfying the following conditions:

- Bilinear: $\forall P,Q \in G$ and $\forall a,b \in \mathbb{Z}, \ \hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$
- Non-degenerate: ∃P₁, P₂ ∈ G that ê(P₁, P₂) ≠ 1. This means if P is generator of G, then ê(P, P) is a generator of Q.
- Computability: there exists an algorithm to compute $\hat{e}(P,Q), \forall P,Q \in G$

Note, some hash functions denoted as follows are also needed: $H_1 : \{0,1\}^* \to G^*, H_2 : \{0,1\}^* \to \mathbb{Z}_q^*, H_3 : \mathbb{Z}_q^* \to \{0,1\}^n$, where the size of the message is defined by n. Apart of this, $a \stackrel{r}{\leftarrow} N$ denotes a selection of an element a randomly from a set $N, a \leftarrow b$ stands the assignation of the value a to b and || is used for concatenation.

The steps used in this signcryption scheme are the following:

SETUP: This step is execute in the base station to the establishment of the basic parameters and to the generation of the base station public key (pk_{bs}) and the base station secret key (sk_{bs}). To achieve this, a prime value q is generated based on some private data k ∈ Z and the system select two groups G and V of order q and a bilinear pairing map ê : G × G → V. P ∈ G is selected randomly and the hash functions H₁, H₂ and H₃ are also chosen.

$$pk_{bs} \xleftarrow{r} \mathbb{Z}_q^*$$
$$sk_{bs} \leftarrow pk_{bs} \cdot F$$

EXTRACT (*ID_r*): In this step, the keys for each robot is generated based on their ID. The robot *r* with the identity *ID_r* sends its information to the base station. The public key *Q_{ID_r}* ∈ *G* and the secret key *S_{ID_r}* ∈ *G* are calculated taking into account the *sk_{bs}*. This key exchange of data is performed in a secure way

$$Q_{ID_r} \leftarrow H_1(ID_r)$$
$$S_{ID_r} \leftarrow sk_{bs} \cdot Q_{ID_r}$$

• SIGNCRYPTION $(S_{ID_{ra}}, ID_{rb}, m)$: If a robot A with the identity ID_{ra} shares a message $m \in \{0,1\}^n$ to the robot B with the identity ID_{rb} , the information will be encrypted and signed. The robot receiver's public key is generated taking into account the ID_{rb} and then the message is signed with $S_{ID_{ra}}$ and encrypted with $Q_{ID_{rb}}$ giving as result σ (a t-uple of three components: c, T, U).

$$Q_{ID_{rb}} \leftarrow H_1(ID_{rb})$$

$$x \leftarrow T_q^*$$

$$T \leftarrow x \cdot P$$

$$r \leftarrow H_2(T||m)$$

$$W \leftarrow x \cdot pk_{bs}$$

$$U \leftarrow r \cdot S_{ID_{ra}} + W$$

$$y \leftarrow \hat{e}(W, Q_{ID_{rb}})$$

$$k \leftarrow H_3(y)$$

$$c \leftarrow k \oplus m$$

$$\sigma \leftarrow (c, T, U)$$

• UNSIGNCRYPTION $(ID_{ra}, S_{ID_{rb}}, \sigma)$: The robot *B* receive σ and parse the information. If everything is right, the message $m \in \{0,1\}^n$ is returned. Otherwise, if there are some problems in the signature or in the encryption of m, \perp is returned. The sender's public key is generated taking into account ID_{ra} and then the message is unencrypted with $S_{ID_{rb}}$.

$$Q_{ID_{ra}} \leftarrow H_1(ID_{ra})$$

$$split \quad \sigma \quad as \quad (c, T, U)$$

$$y \leftarrow \hat{e}(S_{ID_{rb}}, T)$$

$$k \leftarrow y$$

$$m \leftarrow k \oplus c$$

$$r \leftarrow H_2(T||m)$$

Verification:

$$\hat{e}(U,P) == \hat{e}(Q_{ID_{ra}}, pk_{bs})^r \cdot \hat{e}(T, pk_{bs})$$

Note: if the verification is successful m is returned, otherwise \perp is returned.

VI. CONCLUSION

MANET networks allow the connection between different devices and exchange information in a decentralized way. The behavior of such networks is similar to that of a P2P network. The main characteristic of this network is that the different nodes that form it are in motion. In a MANET network with robots, the ability to move nodes remotely is added. In this way it is not necessary to go to the different points where the nodes will be located, but it is possible to move them remotely thanks to streaming video visualization. In addition, the proposal incorporates object tracking, which allows that when moving one of the robots the rest moves behind the first one in an autonomous way.

Using Raspberry Pi as the primary device for each network node gives the system many possibilities. Having a device that runs a Linux operating system gives the possibility to add different services that run for some purpose and the development of applications that may be useful for system users. The USB ports and GPIO pins for device connection provide the possibility of adding different types of sensors for data acquisition or even actuators that can interact with the environment. The low battery consumption of these devices gives the possibility to use a small battery as a power source for these devices, as well as allowing a long use of them before draining the electricity provided by the battery.

In the proposed system, Wi-Fi is used as wireless technology in order to take advantage of the interface that incorporates Raspberry Pi, but it is possible to use any other type of wireless technology, allowing a greater range of coverage, which has an interface that can be connected to Raspberry Pi.

The incorporation of security mechanisms provides added value to the system, so that it can ensure that client devices connected to the generated network are secure. Using Identity-Based Cryptography we are able to provide the information encryption and authentication system by signing, with a low computational complexity.

Apart from the functionality for which this system has been designed, it can be used to perform video surveillance tasks using the camera and microphone incorporated in each of the network nodes, and can be moved thanks to robots to view images from different areas. This can be quite useful in hardto-reach areas, or where people's physical integrity may be at risk.

To improve object tracking, in this case QR codes, in the future the design can be improved by including a small screen in the back of each robot. In this way, the permanent QR code is replaced by a screen that would allow the code to be changed from time to time. This change brings extra security to the system, since every few minutes the code used would become obsolete, thus preventing anyone from being able to move the robots to another location using a QR code that is too old.

ACKNOWLEDGMENTS

Research supported by the Spanish Ministry of Economy and Competitiveness, TESIS2015010102, the European FEDER Fund, and the CajaCanarias Foundation, under Projects TEC2014-54110-R, RTC-2014-1648-8, MTM2015-69138-REDT and DIG02-INSITU.

REFERENCES

- Xi, J., & Bettstetter, C. (2002). Wireless multihop Internet access: gateway discovery, routing, and addressing. Proceedings of 3GWireless, 2.
- [2] Sugiura, Y., Sakamoto, D., Withana, A., Inami, M., & Igarashi, T. (2010, April). Cooking with robots: designing a household system working in open environments. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2427-2430). ACM.
- [3] Bartsch, E. R., Fisher, C. W., France, P. A., Kirkpatrick, J. F., Heaton, G. G., Hortel, T. C., ... & Stigall, J. R. (2002). U.S. Patent No. 6,459,955. Washington, DC: U.S. Patent and Trademark Office.
- [4] Malone-Lee, J. (2002). Identity-Based Signcryption. IACR Cryptology ePrint Archive, 2002, 98.
- [5] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.
- [6] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y. C., & Jetcheva, J. (1998, October). A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking (pp. 85-97). ACM.
- [7] Draves, R., Padhye, J., & Zill, B. (2004, September). Routing in multiradio, multi-hop wireless mesh networks. In Proceedings of the 10th annual international conference on Mobile computing and networking (pp. 114-128). ACM.
- [8] Oda, H., Kulla, E., Ozaki, R., & Nishihara, N. (2016, November). Design of an adhoc testbed for IoT and WSAN applications using Raspberry Pi. In International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 535-546). Springer, Cham.
- [10] Thomas, J., Robble, J., & Modly, N. (2012, November). Off grid communications with android meshing the mobile world. In Homeland Security (HST), 2012 IEEE Conference on Technologies for (pp. 401-405). IEEE.

- [9] Boonsawat, V., Ekchamanonta, J., Bumrungkhet, K., & Kittipiyakul, S. (2010, May). XBee wireless sensor networks for temperature monitoring. In the second conference on application research and development (ECTI-CARD 2010), Chon Buri, Thailand.
- [11] Caballero-Gil, P., Caballero-Gil, C., & Molina-Gil, J. (2013). Design and implementation of an application for deploying vehicular networks with smartphones. International Journal of Distributed Sensor Networks, 9(12), 834596.
- [12] Lodeiro-Santiago, M., Santos-González, I., Caballero-Gil, P., & Caballero-Gil, C. (2017). Secure system based on UAV and BLE for improving SAR missions. Journal of Ambient Intelligence and Humanized Computing, 1-12.
- [13] Kim, G. H., Nam, J. C., Mahmud, I., & Cho, Y. Z. (2016, July). Multidrone control and network self-recovery for flying ad hoc networks. In Ubiquitous and Future Networks (ICUFN), 2016 Eighth International Conference on (pp. 148-150). IEEE.
- [14] Forlizzi, J., & DiSalvo, C. (2006, March). Service robots in the domestic environment: a study of the roomba vacuum in the home. In Proceedings of the 1st ACM SIGCHI/SIGART conference on Human-robot interaction (pp. 258-265). ACM.
- [15] Tribelhorn, B., & Dodds, Z. (2007, April). Evaluating the Roomba: A low-cost, ubiquitous platform for robotics research and education. In Robotics and Automation, 2007 IEEE International Conference on (pp. 1393-1399). IEEE.
- [16] Diddeniya, S. I. A. P., Rathnayake, K. A. S. V., Gunasinghe, H. N., & Wanniarachchi, W. K. I. L. (2017). Integrating iRobot-Arduino-Kinect Systems: An Educational Voice and Keyboard Operated Wireless Mobile Robot. International Journal of Scientific Engineering and Technology, 6(6), 188-192.
- [17] Jardim, E., Bian, X., da Silva, E. A., Netto, S. L., & Krim, H. (2015, April). On the detection of abandoned objects with a moving camera using robust subspace recovery and sparse representation. In Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on (pp. 1295-1299). IEEE.
- [18] Nattharith, P. (2013). Fuzzy logic based control of mobile robot navigation: A case study on iRobot Roomba Platform. Scientific Research and Essays, 8(2), 82-94.
- [19] Buiati, F., Puttini, R., de Sousa, R., Abbas, C. B., & Villalba, L. G. (2004, August). Authentication and autoconfiguration for MANET nodes. In International Conference on Embedded and Ubiquitous Computing (pp. 41-52). Springer, Berlin, Heidelberg.
- [20] Glynos, D., Kotzanikolaou, P., & Douligeris, C. (2005, April). Preventing impersonation attacks in MANET with multi-factor authentication. In Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2005. WIOPT 2005. Third International Symposium on (pp. 59-64). IEEE.
- [21] Umaparvathi, M., & Varughese, D. K. (2010, December). Evaluation of symmetric encryption algorithms for MANETs. In Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on (pp. 1-3). IEEE.
- [22] Lindskog, J., Rydnell, G., & Larsson, P. (2008). U.S. Patent No. 7,443,822. Washington, DC: U.S. Patent and Trademark Office.
- [23] Misra, S., Reisslein, M., & Xue, G. (2008). A survey of multimedia streaming in wireless sensor networks. IEEE communications surveys & tutorials, 10(4).
- [24] Schulzrinne, H. (1998). Real time streaming protocol (RTSP).
- [25] Adobe. Real Time Messaging Protocol (RTMP). "http://wwwimages.adobe.com/content/dam/Adobe/en/devnet/rtmp/pdf/ rtmp_specification_1.0.pdf". [Online; accessed 3-March-2018]
- [26] Yilmaz, A., Javed, O., & Shah, M. (2006). Object tracking: A survey. Acm computing surveys (CSUR), 38(4), 13.
- [27] iRobot Roomba. "http://www.irobot.com/For-the-Home/Vacuuming/Roomba.aspx". [Online; accessed 3-March-2018]
- [28] Wikipedia. Resistive divider. "https://en.wikipedia.org/wiki/ Voltage_divider#Resistive_divider". [Online; accessed 3-March-2018]
- [29] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). Address allocation for private internets (No. RFC 1918).