International Journal of Engineering & Technology, 7 (2.4) (2018) 34-38

International Journal of Engineering & Technology

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

Research Paper

Energy aware approach for security and power optimization in advance wireless networks of internet of things (IoT)

Er. Sharad[1]*, Savita Shiwani[2], Manish Suroliya[3]

[1]Research Scholar, Dept. of Computer Science and Engineering, Jaipur National University Jaipur
[2,3]Associate Professor, Dept. of Computer Science and Engineering, Jaipur National University Jaipur[3]Affiliation of the third author
**Corresponding author E-mail: chasharad@gmail.com*

Abstract

In the recent years, the advance wireless networks and Internet of Things (IoT) are becoming very prominent in assorted domains. In the traffic system, the problem of congestion control is very common, and it is classically handled by the global positioning systems by the drivers as well as traffic administrative authorities. But as the traffic density is increasing day by day, it is becoming difficult to handle and view all the possibilities in the prospective traffic area where the driver is willing to move. Moreover, the problem of security and integrity is also increasing rapidly as there are number of attacks in VANET and GPS systems being used by the crackers by sending the malicious code or fake packets. Ubiquitous computing is one of the recent technologies that is in the phase of implementation under Internet of Things (IoT). 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.

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

1. Introduction

The term Internet of Things was first presented by Kevin Ashton in year 1999. The implementation of IoT is widespread now because of the availability of high performance wireless technologies. Radio Frequency Identification (RFID) tags and Sensors are base in the implementation of IoT. The RFID tags can be embedded in real world devices and objects which can be monitored remotely using software based applications. The RFID readers can be used to locate, read and sense the RFID implanted objects. Very small micro sized transmitting and receiving chips are integrated with RFID which can communicate at distant point. As per the reports from Forbes.com, the market of Internet of Things will reach around 267 billion dollars by year 2020. The analysis from Gartner underlines that around 8.4 billion objects with investment of 273 billion dollars will be interconnected with each other in current year 2017.

RPL (Routing Protocol over Low Power and Lossy Networks)
RPL alludes to the Routing Protocol in view of IPv6 that is implied and concocted towards Low-Power and Lossy Networks. It is taken accepted routing layered convention for the Internet of Things (IoT). From its consistency, RPL added to the advancement of correspondences in the realm of small, inserted, organizing gadgets, by giving, alongside different measures, gauge engineering for IoT. Routing issues are exceptionally trying for 6LoWPAN, given the low-power and lossy radio-interfaces, the battery provided hubs, the multi-bounce work topologies, and the successive topology changes because of portability. Fruitful arrangements ought to consider the particular application necessities, alongside IPv6 conduct and 6LoWPAN systems. A compelling arrangement was created by the IETF Routing Over Low power and Lossy (ROLL) systems working gathering. It has proposed the main IPv6 Routing Protocol for Low power and Lossy Networks (LLNs), RPL, in light of an inclination based approach.

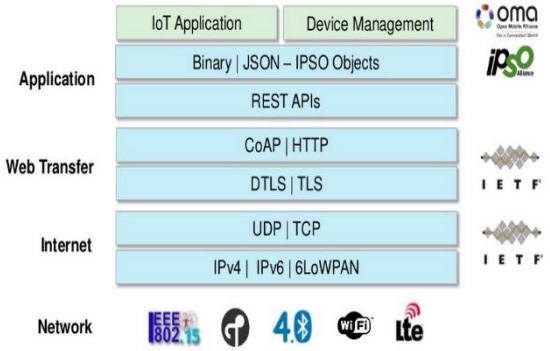

Fig. 1: 6LowPAN Environment

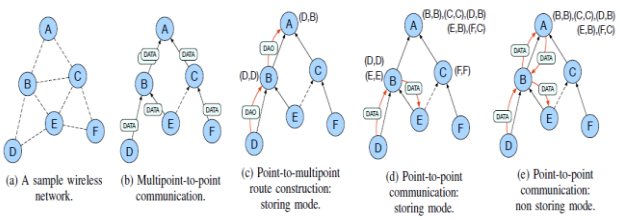

Fig. 2: Routing in RPL. Existing routes are shown next to the network nodes

This problem can arise in RPL when there is inconsistency in the topology. Inconsistency arises due to the congestion, loss of packets or any node failure. RPL enables each node in the framework to pick if packets are to be sent upwards to their family or downwards

to their adolescents. “Routinely, concerning the condition in ContikiRPL that we use to show strikes in this paper, the base troublesome way a node can pick the acquaintance of a packet is with know each one of its relatives which picks the course towards leaf nodes and consider up heading as the default course of a packet. In RPL securing mode, in-structure controlling tables are used to separate packets heading upwards and the packets heading downwards in the framework. RPL has worldwide and interfacing repair parts that can come enthusiastically if there is a controlling topology bewilderment, an association baffled longing, or a node dissatisfaction. On a node (parent) or an affiliation dissatisfaction a zone repair instrument tries to pick another parent or way. In case there are all the more close frustrated desires, RPL plays out a fundamental general repair where the whole DODAG is imitated. The RPL custom uses the conspiracy layer metric as a parameter in the check of a default course. The way is thought to be wonderful if interface layer attestations are gotten on it. RPL in like way uses a stream check to direct peculiarities in the RPL DODAG. Right when a RPL framework is solid, the stream clock break is wide. In any, unending supply of irregularities, the stream clock is reset, and more DIO messages are sent (by the nodes) in the degree of nodes that are subjected to groupings from the standard. The running with events are considered as varieties from the standard in the RPL When arranging circles are seen, When a node joins a DODAG and When a node moves inside a structure and changes rank.

2. Literature Review

A number of researchers and practitioners have worked on the analysis of remote sensor technology and IoT but there is huge scope for the improvement in cases where data transmission & integrity is necessary due to huge requirements of dynamic clustering with confidentiality & integrity.

Table 2.1: Evaluation of Literature Reviewed

Year	Authors	Technology Used	Key Points
2014	Q. Jing et. al	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.
2014	Z. Yan	Trust Architecture and Overall Security Enhancement	The work presents secured multi party computations including privacy preserving database query (PPDQ), Privacy-preserving scientific computations (PPSC), Privacy-preserving intrusion detection (PPID), Privacy-preserving data mining (PPDM) and their association in the IoT scenario.
2014	D. Lake et. al.	IoT in Healthcare	Secured architecture framework with the multilayered approach having key elements of connection, collection, correlation, calculation, conclusion and collaboration.
2014	Y. Ning	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.
2014	M. Turkanovic	Hybrid Authentication	The proposed scheme is having multiple phases including registration phase, login phase, authentication phase, password change phase and dynamic node addition phase. The overall security using proposed mechanism is escalated with factors associated with key agreement, secured mutual authentication, password protection, user anonymity, replay attack, stolen-verified attack, smart card breach attack, impersonation attacks, password change attack, Denial of Service and GWN bypassing attacks.
2015	S. Sicari	Security and Privacy Aware Architecture	Proposed schemes and protocols to make them secured and integrity aware for any type of assault.
2015	J. Granjal	IoT Architecture	In addition, the work in having focus on the protection and security formulations associated with each protocol.
2015	K. T. Nguyen	IPv6 Security	Moreover, the key exchange mechanisms and their relative efficiency along with the security is underlined in this research manuscript.
2015	M. Vucinic et. al.	OSCAR	OSCAR to protect against the replay attacks and security of data channels in the Internet of Things.
2015	W. Trappe	Resource Optimization using Multilayered 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.
2016	F. Li et. al.	Multi-Key Security	Heterogeneous ring based encryption technique to achieve the confidentiality, security, overall integrity and related non-repudiation factors in the network.
2016	S. R. Moosavi	Security with the multidimensional mobility.	The resource optimization factors in this scheme are very effective and achieving the performance and speed to 97%.
2016	K. A. Rehiman	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.
2016	D. Airehrour	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.
2016	E. Bertino	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.
2017	M. Usman et. al.	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.
2017	M. B. Mollah et. al.	Cloud Technologies	The scenario taken here is the Cloud assisted IoT by which the smart objects are able to communicate effectively
2017	P. P. Jayaraman et. al.	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.
2017	C. Schmitt et. al.	Two way solution 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.
2017	S. Prabhakar	Cloud Environment	Vulnerabilities and different susceptibility factors in network and the usage of different mechanisms to avoid these assaults.

3. 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* n *DO*
IF $CH_i \leftarrow$ *Nodes with higher battery power, ability to manage other nodes*
IF (nodes in range of CH*) THEN*
$Transmit\ common\ identifier$
Integration of Nature Inspired Approach Module
Dynamic Key Exchange for Higher Degree of Security and Lifetime
ELSE
The node is under other CH
END IF
END FOR
FOR $i = 0$ *to* n *DO*
IF (source node and destination node is under same CH) 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

Key Points

- Higher level of optimization of energy using Dynamic Cluster Head Selection and Shuffling for unbiased and performance aware approach
- Dynamic topology so that the consistency can be checked and evaluated
- Dynamic Hash Key based Transmission to avoid Energy Consuming Assaults and achieving power and energy aware transmission for escalated lifetime
- The weights and related properties can be set on the real time dynamic network
- Integration of dynamic clustering approaches so that the key can be more secured
- Implementation based on the dynamic clustering can be used for any type of network
- The proposed aspects are effective and giving better results which are the key components of dynamic clustering and overall performance on multiple parameters

4. Implementation and Results

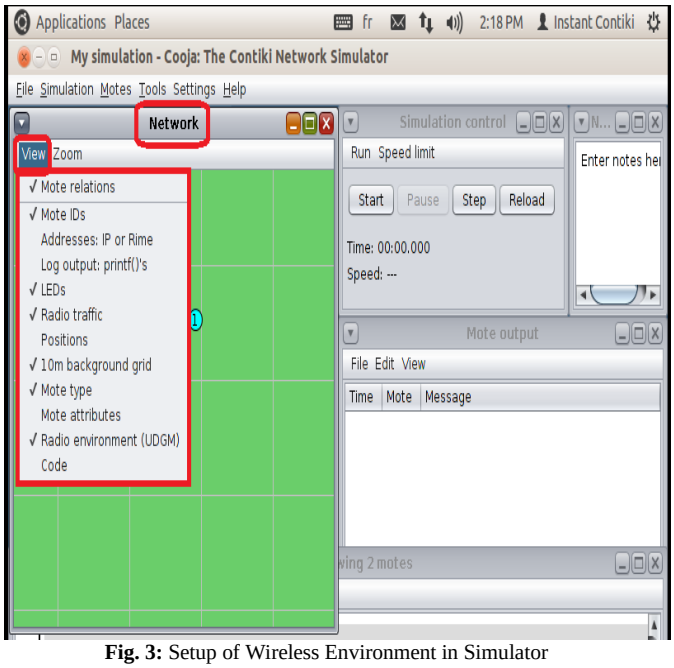

Fig. 3: Setup of Wireless Environment in Simulator

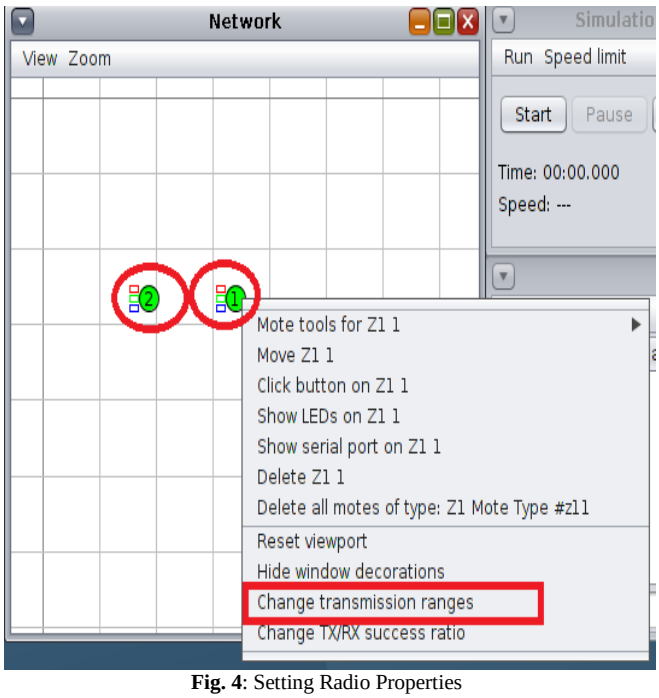

Fig. 4: Setting Radio Properties

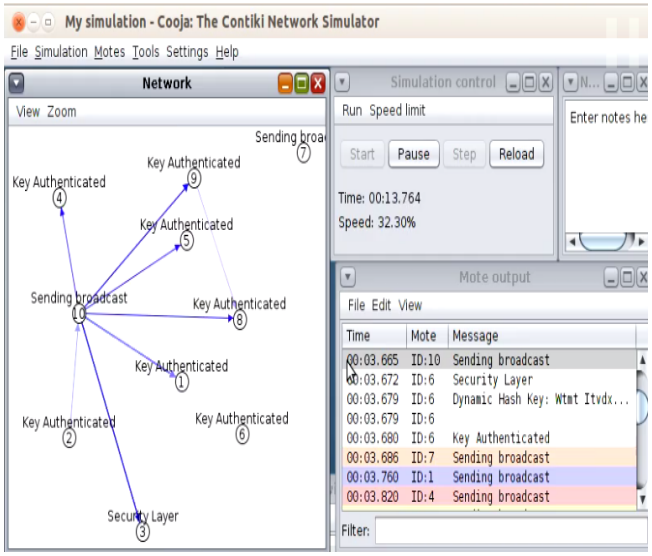

Fig. 5: Elephant Herd Optimization with Key Authentication Process

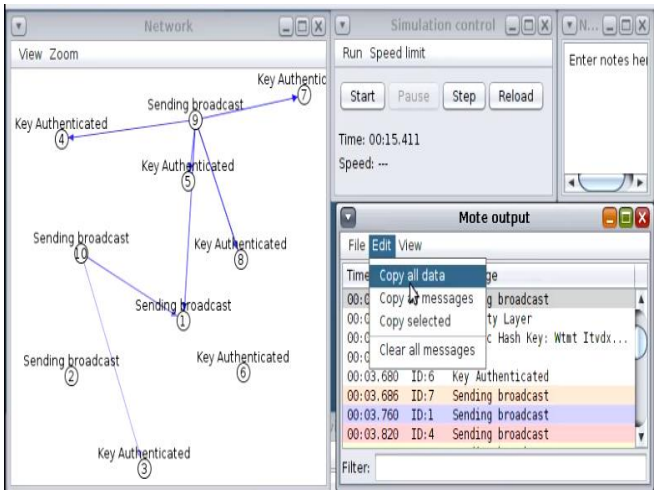

Figure 6 Fetching the data and messages for plotting graphs

Fig. 7: Average Power Consumption in the Motes with VeRA

As depicted in the abovementioned figure, there are enormous parameters including LPM, CPU, Radio Listen and Radio Transmit during the IoT simulation. The graphical results in the above cited graph are consistent and low power mode is in the integrity mode. In addition, the radio listen the having the consistency.

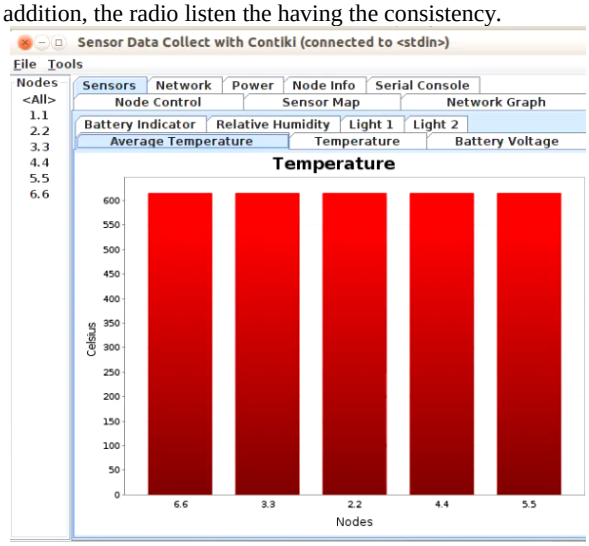

Fig.8: Temperature Evaluation in Celsius at the Motes

The results show that the temperature evaluation and logging aspects are very consistent and integrity aware. The decay of temperatures in the motes is very similar and it shows the consistency in the behavior of the algorithm.

Node	Received	Hops	Rtmetric
1	0	0	0
2	1	1	465
3	1	1	627
4	1	2	821
5	1	1	684
6	2	1	640

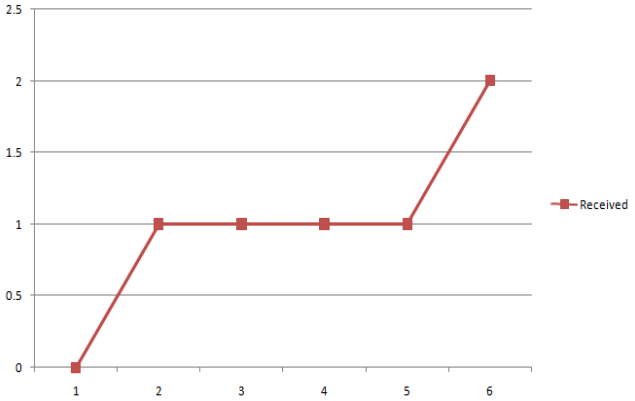

Fig. 9: Logging of received signals by the motes

The abovementioned graph underlines that the logging of received signals by the motes are very effectual and escalating in the network implementations which shows the overall performance and efficiency of the scenario.

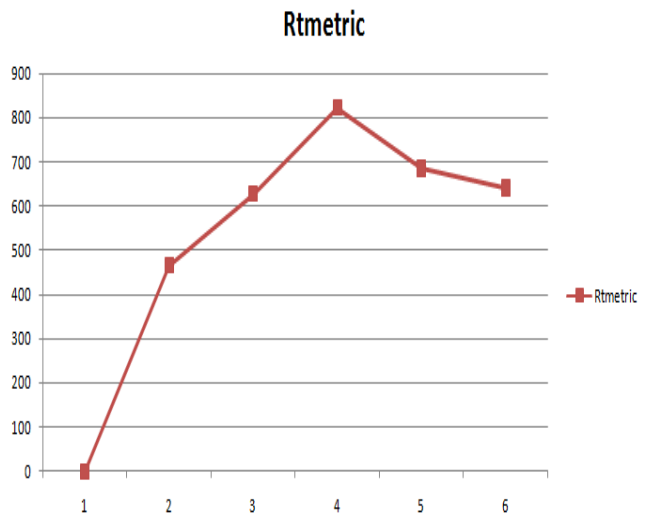

Figure 10 Evaluation of RTmetric after simulation execution

The Router metrics depicted in the above graph and the increasing values depict that the routing is effectual enough to transmit the data in between the motes. In this simulation of IoT network, the scenario of dynamic key exchange between the motes are done in which the dynamic security key is being generated and authenticated for communication. It is necessary to devise and implement the protocols and algorithms by which the overall privacy and performance in communication can be enforced to avoid any intrusion. As IoT can be used for military applications, it becomes mandatory to work on highly secured algorithms of key exchange with dynamic cryptography of security keys. Once the simulation is complete, the network log files are analyzed which includes the source and destination motes, time and overall activities performed during simulation. In the Mote Output Window, the log data can be copied and further analyzed using data mining and machine learning tools for predictive analytics.

5. Conclusion

The use of metaheuristics 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. In this proposed algorithm, efficient routing technique is meant to be followed by various sensor nodes with the help of cluster Heads. 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] A. Zanella, N. Bui, A. Castellani, L. Vangelista and L, Zorzi. Internet of things for smart cities, IEEE Internet of Things Journal. 7 (2014), 22-32.
[2] K. Zhang, X. Liang & X. Shen, Sybil attacks and their defenses in the internet of things. IEEE Internet of Things Journal, 1, 5 (2014) 372-383.
[3] M. Farooq, M. Waseem, A. Khairi. A critical analysis on the security concerns of internet of things (IoT), International Journal of Computer Applications. 9 (2015) 1-7
[4] J. Stankovic. Research directions for the internet of things. IEEE Internet of Things Journal. 10 (2017) 3-9.
[5] O. Said, M. Masud., Towards internet of things: Survey and future vision. International Journal of Computer Networks. 12 (2015) 1-7.
[6] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, Context aware computing for the internet of things: A survey, IEEE Communications Surveys & Tutorials., 15 (2014) 414-454.
[7] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, Security of the Internet of Things: perspectives and challenges, Wireless Networks, 20, 8 (2014) 2481–2501.
[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, 49 (2015) 77–93.
[9] D. Lake, R. Milito, M. Morrow and R. Vargheese, Internet of Things: Architectural Framework for eHealth Security, Journal of ICT, 1, 3 (2014), 301–328.
[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., 8 (2014) 1617–1624.
[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, 20 (2014) 96–112.
[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, 76 (2015) 146–164.
[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, 17 (2015) 1294–1312.
[14] K. Nguyen, M. Laurent, and N. Oualha, Survey on secure communication protocols for the Internet of Things, Ad Hoc Networks, 32 (2015) 17–31.
[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, 12 (2014) 3-16.
[16] W. Trappe, R. Howard, and R. S. Moore, Low-energy security: Limits and opportunities in the internet of things, IEEE Security and Privacy, 13 (2015) 14–21.