Improving WSN Routing and Security with an Artificial Intelligence approach

Sandeep Kumar E

Dept. of Telecommunication Engineering
Jawharlal Nehru National College of Engineering, Shimoga, Karnataka, India
sandeepe31@gmail.com

Abstract. Wireless Sensor Network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment, and organizing the collected data at a central location. Research in WSNs is gaining interest due their different applications and the challenges that the constrained resources of sensor nodes bring on the field. In this type of ad-hoc network, routing of data to the base station with secure transmission is of prime concerns. In this paper, we discuss possible improvements in WSN routing and security through the employment of concepts coming from Artificial Intelligence (AI) area, such as swarm intelligence, artificial immune systems and artificial neural networks. Since WSNs are distributed computing networks, the use of AI makes the network "cognitive" toward solving problems these networks are often prone to.

Keywords. Ad-hoc networks, LEACH protocol, bioinspired computing

1 Routing in Wireless Sensor Networks

WSN architecture is shown in Fig. 1. This network is built of few to several hundreds or even thousands of sensor nodes, where each node is connected to one or several other neighboring nodes. A sensor node will be sensing and delivering the data, the data hops from one node to another node, finally reaching the gateway node based on the routing algorithm used, via gateway node they will be interfaced to the personal computers. Energy efficiency is one of the key challenges of routing data in WSNs. The data has to reach the destination with energy utilization as small as possible. Energy can be related to communication energy overhead, computation energy overhead, etc.

The majority of the research in routing protocols designed for WSNs deals with the node energy efficiency [1]. Routing protocols are broadly classified into flat, hierarchical, and location based. Out of all these protocols, hierarchical protocols have proven to be more energy efficient than the other techniques [2].

In this context, we can design novel clustering protocols using the concepts of AI like swarm intelligence (firefly algorithm [3], glowworm algorithm [4], ant colony optimization [3][24], bee colony algorithm [3], bat algorithm [3]), artificial

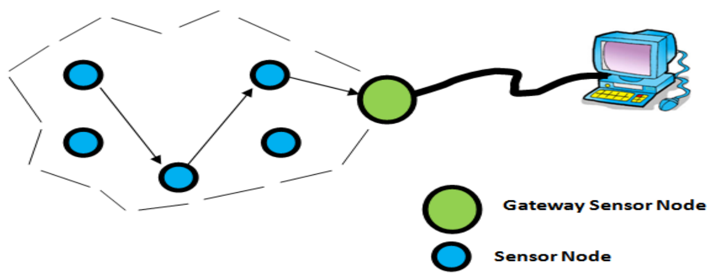

Fig. 1. Wireless Sensor Network

neural networks [5], evolutionary algorithms (genetics [3], memetics [6], etc.) for finding optimal path for data transmission in a network. The proposed routing techniques can be simulated and tested in a standard simulation platform and the results can be compared with the pre-existing protocols like LEACH.

In brief, this section discusses the imitation of grouping behaviors and optimal solution finding technique of living creatures, that can be implemented in WSNs for routing data efficiently to the base station.

2 Security in Wireless Sensor Networks

Research in security is challenging and complex, when compared with other issues related to WSNs [7][25][26][27]. In fact, these networks operate with minimum human intervention, due to which they are prone to additional security threats and vulnerabilities [8]. In this context, we can design novel security techniques for defending against malicious attacks in the network. The proposed ideas for the security in WSNs are described in the following.

A combination of AI with the public keying techniques can be applied for WSNs. The concepts of Artificial Immune Systems (AIS) like negative selection algorithm [9], immune networks [9], danger theory [9], clonal selection algorithm [9] which are basically pattern recognition methodologies can be combined with the random keying techniques (where keys are antibodies against packets which act as antigens) for combating against the security threats. This method can be simulated and tested in standard platforms. The obtained results should be compared with the other widely used keying techniques. This technique combats against some of the security threats like spoofing, denial of service, man-in-middle and sinkhole attacks by confusing the intruder by introducing more randomness in key generation using bioinspired mathematical operations.

A novel approach of inducing the cognitive behavior of vertebrate living organisms is proposed in this paper. This algorithm in a legitimate sensor node takes the randomness of an attacker node into account. The randomness can be related to energy of the attack packet, position of the attacker, strategy of the attacker, so on. For this purpose, the algorithm uses an artificial neural network that is trained according to the previous attack patterns and the strategy, associated payoffs for the picked strategy, and is modeled using game theory. This technique is specially designed to combat against the node capture attack by combining game theory with artificial neural networks. A simulation environment with the malicious attacker, victim node with the proposed algorithm, and the game between them can be modeled and the results can be calibrated.

In brief, this section highlights the usage of AI concepts, to defend against few security threats and attacks. This results in the sensor node being cognitive in handling the security vulnerabilities, especially in remote monitoring and surveillance applications.

3 Related Works

This section discusses few of the works carried in this area. Anthony et al. [10] propose a method to identify the routing path using cuckoo search optimization algorithm. They claim that the path found by the technique is more energy efficient than the existing protocols. The paper uses the brood parasitism of cuckoo birds for optimal path identification. In [11], a novel method for clustering in WSNs is proposed. The paper highlights the usage of social behaviors of Rhesus Macaque monkeys and claim that the method provides energy efficient solution for routing. Sandeep et al. [12] propose a method of clustering for WSNs based on the nest searching strategy of cuckoo bird. Vikram [13] proposes the usage of bacterial foraging technique as an optimization strategy for clustering of sensor networks. In [14], a technique is proposed, which uses firefly's light flashing behavior for clustering in wireless sensor networks. Bharathi et al. [15] discusses the usage of elephant's swarm optimization technique for efficient data aggregation in wireless sensor networks. Eshan et al. [16] propose efficient routing protocol based on the combination of ant colony optimization with fuzzy techniques. Hosein et al. [17] propose a technique of securing WSNs using ant colony optimization for finding a trustable path for communication. Heena et al. [18] discuss a method of imitating the immune system of vertebrates. It combines the concept of AIS with machine learning technique to defend against the malicious packets. Wei- Ren et al. [19] propose a bio- inspired technique using the self- organizing neural networks with competitive learning for security in WSNs. Suman et al. [20] propose a technique of securing clustered sensor networks using random keying technique with memetic operators. Matthias et al. [21] discuss a technique that combines AIS with Bayesian classifier for intrusion detection. In [22], a method of using random keying techniques with AIS for detecting spoofed packets in hierarchical wireless sensor networks is proposed.

Still there are many research works, which adapt bioinspired computation for solving issues of wireless sensor networks; in this paper, we discuss majorly the usage of artificial intelligence to solve routing and security related issues of WSNs.

4 Novelty in the proposal

In one of our previous works [14], we proposed an algorithmic approach of using Rhesus Macaque animal's social behavior for energy efficient clustering in WSNs, which includes the wandering behavior of male monkeys, splitting of monkey groups, choosing of group heads and queens, etc. In this context, we can further study the behaviors of other living creatures and extract intelligent patterns that can be adapted for solving issues of WSNs effectively. In addition, existing nature inspired optimization algorithms can be modified such that it can be adapted for the resource constrained sensor nodes. In the majority of the research works, the optimization algorithm is performed by special type of sensor nodes called the anchor nodes [23]. They perform the operation of choosing the cluster heads and disseminating the information. This increases the deployment cost. Instead, if optimization algorithms are made to execute in all the sensor nodes, the nodes may exhaust the resources due to burden of computation, memory and storage. Hence, we can obtain solution for this problem by adapting optimization algorithms, such that it can be executed only once with a notion of choosing a cluster head, and forming clusters of their own in WSN environment [12]. This might not lead to optimal cluster head choice, but may approximate and a tradeoff can be brought in. Hence, these algorithms can serve as light weighted protocols best suitable for sensor network applications.

According to the survey, majority of the concepts related to AI like AIS, ANNs, combinations between them, etc. have been applied for wireless sensor networks. Nevertheless, still the concepts of evolutionary algorithms like genetics, memetics and AIS concepts like Negative Selection Algorithm, Dendritic cell theory, etc. can be combined with keying techniques (public, private, random, so on) to improve the strength of cryptographic algorithms, trust and security protocols. In our previous work, we have attempted few of the AI derived techniques [20][22][28]. However, still many research works can be carried out in this context.

The strategy making capability of vertebrates to achieve a given task can be implemented in sensor nodes. This is achieved by combining game theory with machine learning algorithms. Here game theory helps in modeling different strategies of the individuals with their associated payoffs. The use of machine learning helps in visualizing the attack scenario. Implementation of this concept leads to a cognitive system that can think and act based on the attacks with its associated intruder strategies. Games like noncooperative, repetitive, Bayesian, cooperative combined with the machine learning concept leads to a novel approach towards securing WSNs.

Here, we can notice three things, the usage of artificial intelligence in clustering, cryptographic keys to immune and secure their communications when attempted for sinkhole attack, hello flood attack, spoofing attack and so on. To provide additional security against the node capture attack one can opt for the combination of game theory with machine learning techniques [29].

We can implement the above routing and security concepts in every sensor node of the deployed network as a protocol stack. By this, we can make sen-

sor nodes behave more intelligently to group, secure communication and combat against the attack if intrusion sustains with less help from Base Station. The combination of all these may lead to a "cognitive sensor network" not with the notion of having cognitive radio in it, but the nodes which are having the capability to visualize and take actions on its own in the absence of manual monitor.

5 Defense Mechanism for Security in WSN using Game Theory and ANN

This paper discusses the applications of bio- inspired computation towards solving the issues and challenges of WSNs. As an example, a novel method of securing WSN against node capture attack is explained in detail. The section highlights a technique of imitating cognitive behavior of vertebrates while defending against attacks. As introduced before in section 2 and section 4, this is achieved by combining game theory with artificial neural networks. Game theory is used for modeling the strategic moves of victim node and attacker node while, ANN is used as pick and play tool by learning the attacker. The proposed methodology can be applied when a malicious intruder is trying for a node capture attack. A node capture attack is defined as an attack where the attacker captures a node and hacks the critical information (eg., cryptographic algorithms) residing in the node. The defense mechanism module is shown in Fig 2. This module is designed to be built in every sensor node, which can combat against such attacks, with minimal help from Base Station. An adversary is assumed to attack any victim node by sending malicious packets to hack the information in the victim node. Intruder node is assumed mobile with its attack packet bit energy varying, such that the intruder's mobility and bit energy of attack packet is highly random in nature. Even, the attacker's strategy is random.

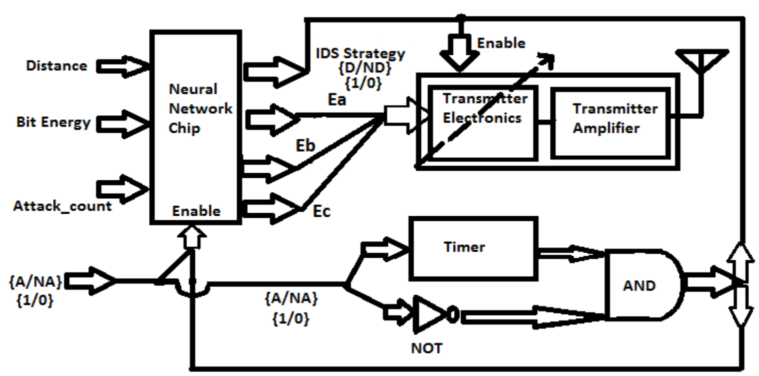

Fig. 2. Intruder Defense Mechanism (IDS)

The proposed Intruder Defense System (IDS) has to be installed in a sensor node as an add-on application together with a cryptographic algorithm. The system will be ignited if number of erroneous packets detected by cryptographic scheme crosses beyond a particular threshold. IDS once ignited continuously combats against a malicious intruder until the game between the intruder and the victim reaches a zero sum game i.e., either intruder stops sending poison packets or dies losing its battery power or victim node is infected or dies losing its battery power.

The module consists of an ANN, whose inputs are distance, bit energy, attack_count and attacker_strategy. Distance input of ANN is defined as the distance between the attacker and the victim, which is the information sent by the BS from time to time until the game exists. Bit energy input is the energy per bit of the poison packet reaching the victim node. attack_count input is the previous attack counts from that intruder under vigilance, which will be updated from time to time. Apart from these, the neural network chip will be enabled only if the attacker's strategy is in attack mode. The output of the neural network is a decision depending all these inputs fed. It can be either to defend or not defend, depending on which the transmitter module will be enabled, and its transmitting energy per bit of the defense packet will be varied according to the scenario.

In Figure 2, there is a timer module, which monitors the intruder and initiates counter attack when the intruder is idle for a long time. This type of attack repeats for few times and stops if the intruder quits its attack.

5.1 Game theoretic modeling

Game theory is a mathematical concept, which deals with the formulation of the correct strategy that will enable an individual or entity when confronted by a complex challenge to succeed in addressing that challenge.

Proposed game model The method proposed is a non-cooperative game between a malicious node and the IDS. The action set of malicious node is $A_m = \{A, NA\}$ and that of IDS is $A_I = \{D, ND\}$ the game ends if either of the one seizes its operation, leading to zero-sum game. Table 1 gives the payoff matrix. The move chosen by IDS solely depends on the accuracy of Neural Network design. E1 is the utility cost for the IDS on reception of an intruder packet

Table 1. Payoff Matrix

	INTRUDER		
IDS		Attack(A)	Not Attack (NA)
	Defend (D)	E1, E2	E5, E6
	Not Defend (ND)	E3, E4	0 , 0

and is given by

$$E1 = (E_{rx} * I) + (E_{pro} * I) + (E_{tx} * A) + (E_{amp} * A * d^n) \tag{1}$$

'I' is the packet sent by the intruder and 'A' is the alarm packet used to counter attack intruder by the victim node. Epro is the energy for processing the intruder packet including the computation energy of the neural network, n is the path loss component.

$$E2 = (E_{rx} * A) + (E_{pro} * A) + (E_{tx} * I) + (E_{amp} * I * d^n) \tag{2}$$

If IDS chooses not to defend while the intruder is on attack then the utility cost is given by

$$E3 = (E_{rx} * I) \tag{3}$$

$$X = X - X_C \tag{4}$$

$$E4 = (E_{tx} * I) + (E_{amp} * I * d^n) \tag{5}$$

Where, X_C is the damage cost of the node for choosing not to defend when the intruder is on attack. X is the residual cost of the victim node. The value of X_C is decided by the amount of damage done by the intruder on the victim node, by hacking information, changing frequency, so on. If Intruder chooses not to attack if IDS is on defense, then the payoff is given by

$$E5 = (E_{rx} * A) \tag{6}$$

$$Y = Y - Y_C \tag{7}$$

$$E6 = (E_{tx} * A) + (E_{amp} * A * d^n) \tag{8}$$

Y_C damage cost of intruder for not attacking the victim node, while the IDS is in defense. Y is the residual cost of the intruder. If intruder chooses not to attack and if IDS chooses not to defend then the utility cost for each is 0. Apart from these payoffs, an intruder has to spend energy in listening all the nodes in network and attacking a node. If P_l is the power consumed per second for listening then, the overall energy consumed by the intruder for listening N number of nodes, is given by

$$E_{listen} = P_l * t * N \tag{9}$$

Where, t is the time dedicated by intruder in listening to each node, N is the total number of nodes in the network and it should be noted that intruder details are unknown to the defender. In the proposed game {ND, NA} is the Nash equilibrium condition. {D, A} is the Pareto optimal strategy for the entire game. In specific {ND, A} is the Pareto Optimality for an intruder and {D, NA} is the Pareto Optimality for IDS.

The efficiency of the game depends entirely on the accuracy of the ANN. The game discussed in this method is a non- cooperative game. Similarly, we can adapt a Bayesian game, repetitive game, so on. For the deployment of this module in a sensor node, ANN has to be pre trained with these type of attacks, which might have happened prior in a network. Implementing this technique in sensor node makes it to self defend against the malicious node attacks in WSNs.

Table 2. Training Matrix 1

Intruder Strategy (ENABLE input for NN)	Count, C	Distance b/w attacker and victim, (d0)	Bit Energy of the attacked packet	Output Strategy	Output Energy	Target set
Attack	$C1 < C \leq C2$	$< d$	$E1 < E0 \leq E2$	Defend	Ea	[1 1 0 0]
Attack	$C1 < C \leq C2$	$< d$	$E2 < E0 \leq E3$	Defend	Eb	[1 0 1 0]
Attack	$C1 < C \leq C2$	$< d$	$E3 < E0 \leq E4$	Defend	Ec	[1 0 0 1]
Attack	$C1 < C \leq C2$	$< d$	$E0 < E1$	Not Defend	–	[0 X X X]
Attack	$C1 < C \leq C2$	$< d$	$E0 > E4$	Defend	Ea Default	[1 1 0 0]
Not Attack	$C1 < C \leq C2$	X	X	Not Defend	Unchanged	[1 1 0 0]

Neural Network and its associated training matrices Artificial Neural Networks are the imitations of biological neural networks. It accepts finite set of inputs and computes the weighted sum. The sum is compared with suitable threshold. The summation and threshold unit is called a node in ANN. Always a NN requires training and is the most difficult task, where we find the weights that achieve goal with acceptable performance. For the proposed work, we use NN with 3 neurons in the input layer, few neurons in the hidden layer and 4 neurons in the output layer. Neurons in the hidden layer depend solely on the cost and the accuracy of ANN. Well-known back- propagation algorithm can be used for training. This is an example implementation and other variants of ANN can be implemented.

An example Training matrix is shown in Table 2. X indicates 'do-not care' condition. E1, E2, E3, E4 are the assumed extremes, dividing the received bit energy levels of the intruder into three classes. C1, C2, C3, C4 are the extremes dividing the count input, fed to the IDS. C1 and c2 are used in Table 2, by considering C3 and C4, and conditions $d0 = d$ and $d0 > d$, remaining conditions for training NN can be derived. C is the intruder's previous attack count, d is the initial distance between attacker and the victim node and d0 is the randomly changing distance between them. It is to be noted that, the output energy level indicators are restricted for four levels. For still better design, we can opt for more level indicators, but with a tradeoff of more neurons requirement rendering increase in the complexity of the design. In addition, the input count can be still divided into a finer class for better combat, but with the tradeoff with the complexity of ANN design.

6 Conclusions

In this paper we discuss about possible approaches of using Artificial Intelligence in handling issues of WSNs like energy consumption in data transmission for efficient routing and security in WSNs—while making the network cognitive towards handling the challenges arising while in operation. The concepts discussed in this paper direct the researchers for the use of bioinspired computation toward solving problems of WSNs by making sensor nodes more intelligent.

References

1. Chelbi S., Abdouli M., Bouaziz R., Duvallet C.: Multi-hop Energy Efficient routing protocol based on Data Controlling for Wireless Sensor Networks. International Conference on Computer Systems and Applications (AICCSA),pp 1–6 (2013)
2. Qiang Do, Aihua Shao, Kang Zhu, Peisi Chu, Yonghua Xiao, Yunfeng Peng, Keping Long: An energy efficient routing protocol for Wireless Sensor Network. 18th Asia-Pacific Conference on Communications (APCC),pp 823–827 (2012)
3. Xin-She Yang: Nature- Inspired Metaheuristic Algorithms. Luniver press, (2010)
4. Krishnanand K. N., Debasish Ghose: Glowworm swarm optimization for simultaneous capture of multiple local optima of multimodal functions. Journal of Swarm Intelligence,pp 87–124 (2009)
5. Mohamad H Hassoun: Fundamentals of artificial neural networks. MIT Press, (1995)
6. Moscato Pablo: On evolution, search, optimization, genetic algorithms and martial arts: Towards memetic algorithms. Caltech concurrent computation program, C3P Report 826, (1989)
7. Shigen Shen, Guangxue Yue, Qiying Cao: A Survey of Game Theory in Wireless Sesnor Networks Security. Journal of Networks, Vol. 6(3),pp 521–532 (2011)
8. Patel M.M., Aggarwal A.: Security attacks in wireless sensor networks: A survey. IEEE International Conference on Intelligent Systems and Signal Processing (ISSP),pp 329–333 (2013)
9. Jason Brownlee: Clever Algorithms: Nature-Inspired Programming Recipes, (2011)
10. Anthony Arul Raj D., Sumathi P.: Enhanced Energy Efficient Multipath Routing Protocol for Wireless Sensor Communication Networks using Cuckoo Search Algorithm. Wireless Sensor Networks, 6, pp 49-55 (2014)
11. Sandeep Kumar E., Kusuma S M., Vijaya Kumar B.P.: Clustering Protocol for Wireless Sensor Networks based on Rhesus Macaques (Macaca mulatta) Animal's Social Behavior. International Journal of Computer Applications (IJCA), Vol. 87 (8), pp 20-27 (2014)
12. Sandeep Kumar E., Mohanraj G.P., Raghuchandra R. Goudar: Clustering Approach for Wireless Sensor Networks based on Cuckoo Search Strategy. International Journal of Advanced Research in Communication and Computer Engineering (IJARCCE), Vol. 3(1), pp 92-95 (2014)
13. Vikram Dhiman: Bio- Inspired Hybrid Routing Protocol for Wireless Sensor Networks. International Journal for Advance Research in Engineering and Technology, Vol. 1(4), pp 33-36 (2013)
14. Sandeep Kumar E., Kusuma S M., Vijaya Kumar B.P.: Fire- LEACH: A Novel Clustering Protocol for Wireless Sensor Networks based on Firefly Algorithm. International Journal of Computer Science: Theory and Applications (IJCSTA), Vol. 1(1), pp 12-17 (2014)
15. Bharathi M.A., Vijaya Kumar B.P., Manjaiah D.H.: Cluster based Data Aggregation in WSN using Swarm Optimization Technique. International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2(12), pp 140-144 (2013)
16. Eshan Amiri, Hassan Keshavarz, Mojtaba Alizadeh, Mazdak Zamani, Touraj Khodadadi: Energy Efficient Routing in Wireless Sensor Networks based on Fuzzy Ant Colony Optimization. International Journal of Distributed Sensor Networks, Vol. 2014 (2014)

17. Hosien Marzi, Mengdu Li a: An Enhanced Bio- Inspired Trust and Reputation Model for Wireless Sensor Networks. Proc. of 4th International Conference on Ambient Systems, Networks and Technologies, Procedia of Computer Science, Vol. 19, pp 1159-1166 (2013)
18. Heena Rathore, Venkataramana Badaria, Sushmitha Jha, Anupam Gupta: Novel Approach for Security in Wireless Sensor Network using Bio- inspiration. Proc. of 6th International Conference of Communication Systems and Networks (COMSNETS), IEEE, Indian Institute of Science, Bangalore, pp 1-8 (2014)
19. Wei Ren, Jun Song, Zhao Ma, Shiyomg Huang: Towards a Bio- inspired Security Framework for Mission- Critical Wireless Sensor Networks. Computational Intelliegence and Intelligent Systems, Communications in Computer Science and Information Science, Vol. 51, pp 35-44 (2009)
20. Suman S.B., Ranjith Kumar P.V., Sandeep Kumar E.: Random Keying technique for Security in Wireless Sensor Networks based on Memetics. International Journal of Computer Science: Theory and Applications, Vol. 1(2), pp 25-31 (2014)
21. Matthias Becker, Martin Drozda, Sven Schaust, Sebastian Bohlmann, Helena Szczerbicka: on Classification Approach for Misbehavior Detection in Wireless Sensor Networks. Journal of Computers, Vol. 4(5), pp 357-365 (2009)
22. Sandeep Kumar E., Kusuma S.M., Vijaya Kumar B.P.: A Random Key distribution based Artificial Immune System for Security in Clustered Wireless Sensor Networks. Proc. of 2nd IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), MANIT, Bhopal, Madhya Pradesh, India (2014)
23. Haojun Huang, Guangmin Hu, Fucai Fu: Energy-aware geographic routing in wireless sensor networks with anchor nodes. International Journal of Communication systems, Vol. 26(1), pp 100-113 (2013)
24. Reza Khoshkangini, Syroos Zaboli, Mauro Conti: Efficient Routing Protocol via Ant Colony Optimization (ACO) and Breadth First Search (BFS). In Proceedings of the IEEE International Conference on Cyber, Physical and Social Computing (IEEE CPSCom 2014), in press, Taipei, Taiwan, September 1-3 (2014).
25. Conti M., Di Pietro R., Mancini L. V.: Secure cooperative channel establishment in wireless sensor networks. In Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (IEEE PerCom 2006 workshop: PerComW 2006), pages 327-331, Pisa, Italy, March 13 (2006)
26. Mauro Conti, Roberto Di Pietro, Angelo Spognardi: Wireless Sensor Replica Detection in Mobile Environments. In Proceedings of the 13th International Conference on Distributed Computing and Networking (ICDCN 2012), Hong Kong, January 3-6, pages 249-264 (2012)
27. Sankardas Roy, Mauro Conti, Sanjeev Setia, Sushil Jajodia: Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact. In (IEEE) Transactions on Information Forensics & Security, 9(4): pages 681-694 (2014)
28. Andrea Gabrielli, Luigi V. Mancini: Bio-Inspired Topology Maintenance Protocols for Secure Wireless Sensor Networks. , In Proc. of the Bio-Inspired Computing and Communication: 1st Workshop on Bio-Inspired Design of Networks (Biowire 2007), Cambridge, UK, April (2007)
29. Emmanouil Panaousis, Tansu Alpcan, Hossein Fereidooni, Mauro Conti: Secure Message Delivery Games for Device-to-Device Communications. In Proceedings of the 5th Conference on Decision and Game Theory for Security (GameSec 2014), pages 195-215, Los Angeles, CA, USA, November 6-7 (2014).