BIOSARP: Biological Inspired Self-Organized Secure Autonomous Routing Protocol for Wireless Sensor Network

Kashif Saleem, Norsheial Fisal, Sharifah Hafizah
Faculty of Electrical Engineering
Universiti Teknologi Malaysia
81310-Skudai, Malaysia
{kashif_pg, sheila}@fke.utm.my http://trg.fke.utm.my

Abstract—In multihop wireless sensor networks users or nodes are constantly entering and leaving the network. Classical techniques for network management and control are not conceived to efficiently face such challenges. New mechanisms are required, to work in a self-organized manner. The techniques found in nature promises WSN, to self-adapt the environmental changes and also self-protect itself from the malicious stuff. This paper introduces a biological inspired self-organized secure autonomous routing protocol (BIOSARP). Our proposed protocol is based on ANT Colony System (ACS) for an optimal route decision. The self-optimized routing protocol is further enhanced with artificial Immune System (HIS) inspired autonomous security mechanism. It enhances WSN in securing itself from the abnormalities and most common WSN routing attacks. NS2 based simulation analysis and results of BIOSARP are presented. The comparison of our autonomous protocol with the most recent WSN security mechanisms is further exhibited, in terms of processing time, delivery ratio and energy consumption.

Key-Words- ANT Colony system, Artificial Immune system, Human Immune Blood Brain Barrier System, Human Immune System, Self-Optimization, Self-Security, Wireless Sensor Network.

1 Introduction

Wireless communication plays an important role in telecommunication sector and has huge importance for future research. The communication is making the world's life easier with the development of sensing and monitoring systems. In these sensing and monitoring systems new gadgets and software advancement are frequently available to the end-user. In infrastructure less networks such as WSN, the deployment area may be out of human reach. The challenges such as growing complexity, unreachable maintenance and unsecure communication demand for mechanism that can maintain the features of WSN such as multihop routing in dynamically changing environmental in a complete autonomous mode. In order to address autonomous capability for multihop ad-hoc network, it has been visualize that self-organized and self-secure network application can fully realize the network operational objectives.

Probabilistic methods that provide scalability and preventability can be found in nature and adapted to technology. Towards this vision, it is observed that various biological principles are capable to overcome the above adaptability issues. The most well-known bio-inspired mechanism is the swarm intelligence (ANT Colony, Particle swarm), AIS and intercellular information exchange (Molecular biology)[1-4]. Many of ant-based ad-hoc network routing algorithms have been presented, such as AntHocNet [5], EARA [6], ANSI [7], ARAMA [8, 9], AOER [10]. Beside these ant-based algorithms, bee inspired algorithms such as BeeAdHoc [11], BiSNET/e [3] have been reported. [4] propose misbehavior detection in nature inspired MANET protocol, BeeAdHoc. However, self-healable security is still an open issue. Widespread acceptance and adaptation of these protocols in real world wireless networks would not be possible until their security aspects have thoroughly investigated [4].

Bio-inspired autonomous routing protocol (BIOARP) that utilizes ANT Colony Optimization (ACO) for the optimum route discovery in WSN has already been presented in [12-14]. In this paper we propose **BIO**logical **I**nspired Self-organized **S**ecure **A**utonomous **R**outing **P**rotocol (BIOSARP) that consists of an

This work supported in part by the Faculty of Electrical Engineering, University Technology Malaysia.

additional self-security management module on top of BIOARP.

BIOSARP is based on the behaviour of human immune system (HIS). As HIS provides the complete security and protection to human body. The major aspect of HIS is to detect the anomalies by differentiating between self and non-self entities. The HIS security is used in the computer world with the name of artificial immune system (AIS).

General AIS algorithms are very complex and impracticable for WSN. The proposed AIS for BIOSARP algorithm is the extension of SAID [15] and BeeAIS [4]. While implementing BIOSARP, the complexity factor is taken under consideration. Moreover, the human immune barrier system is enabled in BIOSARP in the initialization and learning period. These techniques will be accomplished by assigning each procedure to several groups of agents. These agents will work in a decentralized way to collect data and/or detect an event on individual nodes and carry data to the required destination. BIOSARP provides autonomous security, the mechanism overcome the message alter, wormhole, sinkhole Sybil, selective forwarding and HELLO flood attacks.

The next section reviews the related research for optimum route discovery through ACO, self-security using AIS and keying based security approaches. Section 3 describes the BIOSARP architecture. Section 4 shows the implementation, results and comparison. The conclusion and future work are discussed in section 5.

2 Related Research

2.1 Overview of ACO based Routing in WSN

Ant colony algorithms were first proposed by Dorigo et al [16] as a multi-agent approach to solve difficult combinatorial optimization problems like the traveling salesman problem and the quadratic assignment problem, and later introduced the ACO meta-heuristic.

ACO algorithms are a class of constructive meta-heuristic algorithms that mimic the cooperative behavior of real ants to achieve complex computations and have been proven to be very efficient to many different discrete optimization problems. Many theoretical analyses related to ACO show that this optimization can converge to a global optima with non-zero probability in the solution space [17] and their performance have greatly matched many well-studied stochastic optimization algorithms, for example, genetic algorithm, pattern search and annealing simulations [18]. This paper is particularly on BIOSARP autonomous security module. The ACO based routing BIOARP has been discussed in detail previously in [12, 14, 19].

2.2 Security in WSNs

Wireless sensor nodes are mostly deployed in the unprotected/hostile environment. Therefore, it is easier for WSN to suffer with a number of attacks, due to sensor nodes resource constraints and vulnerabilities. These attacks involve signal jamming and eavesdropping, tempering, spoofing, resource exhaustion, altered or replayed routing information, selective forwarding, sinkhole attacks, Sybil attacks, wormhole attacks, flooding attacks and etc [20]. Many papers have proposed prevention countermeasures of these attacks and the majority of them are based on encryption and authentication. These prevention measures in WSN can reduce intrusion to some extent. In this case, intrusion detection system (IDS) can work as second secure defence of WSN to further reduce attacks and insulate attackers.

2.2.1 Overview of AIS based Self-Security in WSN

In [15], the authors have proposed SAID with three-logic-layer architecture. SAID adopt the merits of local, distributive & cooperative IDS and is self-adaptive for intrusion detection of resource-constraint WSN. Knowledge base is deployed base station where the complex algorithm for agent evolution can be computed and intrusion rules can be stored.

[21] proposed a new group-based intrusion detection scheme. In this scheme, the authors partition the sensor nodes in a network into a number of groups. The nodes in a group have the same sensing capability and are physically close to each other. The proposed intrusion detection algorithm is scheduled to run for each group. Through experiments in which the authors use data released from the Intel Berkeley Research Lab, he has shown that their scheme can achieve a lower false alarm rate and a higher detection accuracy rate than the present intrusion detection schemes and would consume less power.

Most IDS for internet network or mobile Ad Hoc network cannot be applied in WSN mainly due to the resources constraint in WSN. Therefore, there are many challenges as the implementation of IDS in WSN are still at the beginning [15]. [15] shows that the operation of BeeHive algorithm requires an initialization phase (30 seconds) before the AIS learning could start. It is

ISBN: 978-1-61804-039-8

followed by the learning (50 seconds) and protection phases to respectively learn the BeeHive normal behavior and detect the routing attacks [4].

2.2.1 Overview of keying based Security in WSN

Due to the factor of initialization phase, WSN need security mechanism to be in operation before the network deployment. As stated in [22] Node cloning attacks can be mounted only during deployment since a cloned node cannot initiate the protocol with success. It can be successfully connected only by acting as a responding node. Recent progress in implementation of elliptic curve cryptography (ECC) on sensors proves public key cryptography (PKC) is now feasible for resource constrained sensors [23]. The performance of PKC based security schemes is still not well investigated due to the special hardware characteristics.

In [24] a scheme has been proposed which explores the superimposed s-disjunct code for a timely clone attack detection. A fingerprint can be easily encoded with a very short bit stream, which results in small message overhead.

In [25] the author presents the security enhancement which uses encryption and decryption with authentication of the packet header to supplement secure packet transfer. SRTLD solves the problem of producing real random number problem using random generator function encrypted with mathematical function. The output of random function is used to encrypt specific header fields in the packet such as source, destination addresses and packet ID. In this mechanism they assume that each sensor node is static, aware of its location and the sink is a trusted computing base.

A pairwise key establishment (PKE) based on transitory master keys as discussed in [22] is particularly useful for the coding purpose. LEAP++ consists of system setup, pairwise key establishment and authentication key disclosure.

Security in natural inspired routing protocols is still an open issue [4]. Widespread acceptance and adoption of these protocols in real world wireless networks would not be possible until their security aspects have thoroughly been investigated.

3 Methodology

3.1 BIOSARP Self-Security Architecture

BIOARP is enriched with a autonomous security management; preliminary work is given in [26]. The AIS mechanisms mentioned above [21] [15] are very complex and their algorithms are huge for WSN. These mechanisms also need enormous database to maintain knowledge. We have divided the jobs among the agents. Agent works on two-layered architecture, agent layer on the top and wireless sensor network on bottom as shown in Fig 1. The agent layer contains three types of agents, which are monitoring, decision and defence.

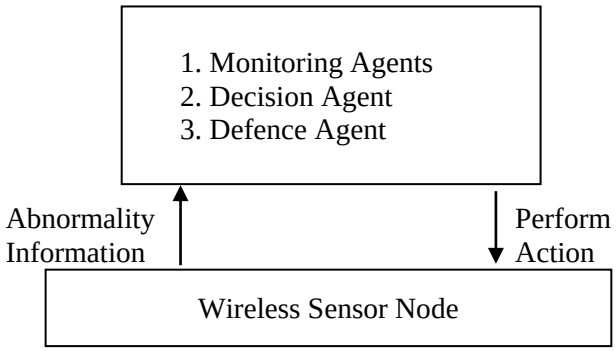


Fig 1. Two layer BIOSARP Self-Security Architecture

The autonomous security module cooperates with the routing management, neighbour management and power management modules to provide self-organized secure autonomous routing protocol for WSN. Whenever the neighbour table is checked to select the optimal node, the neighbouring node behaviour is monitored in the routing management. As soon as the abnormal behaviour is detected, the information is delivered or passed to the security management module. The security management module then matches the neighbouring node characteristics with the given threshold. If there is any neighbouring node mismatches, the security module classifies it as non-self. After classification, the security module sends the appropriate action command to routing management as given in Fig 2.

The flow of the system is elaborated with the help of flowchart as shown in Fig 3. Whenever routing management module wants to select the next best node, the monitoring agent checks the behaviour of neighbouring nodes. First, the numbers of records are counted in neighbour table. If no record is found the checking process is deferred until the neighbours are discovered. Otherwise, the behaviour checking continues with the initialization of variables as shown in Table 1. After initialization the correlation coefficient function is called which determines the relationship difference between x and y arrays. The correlation coefficient is a statistical function as shown by Equation 1 to calculate the relation between two groups of same entity. The statistical matching rule produces a number between -1 and 1 that relates how similar the two input sequences are.

ISBN: 978-1-61804-039-8

Table 1. Security Parameters

	Packet Receiving Rate	***Energy***		***Packet Mismatch Rate***	***Packet Receiving Rate***
Tackled Attacks	Sink hole attack [21]	To make relationship with		Message alter attack[21]	To make relationship with
Node 1	x_1^1	y_1^1		x_2^1	y_2^1
Node 2	x_1^2	y_1^2		x_2^2	y_2^2
.	.	.		.	.
.	.	.		.	.
.	.	.		.	.
.	.	.		.	.
Node n	x_1^n	y_1^n		x_2^n	y_2^n

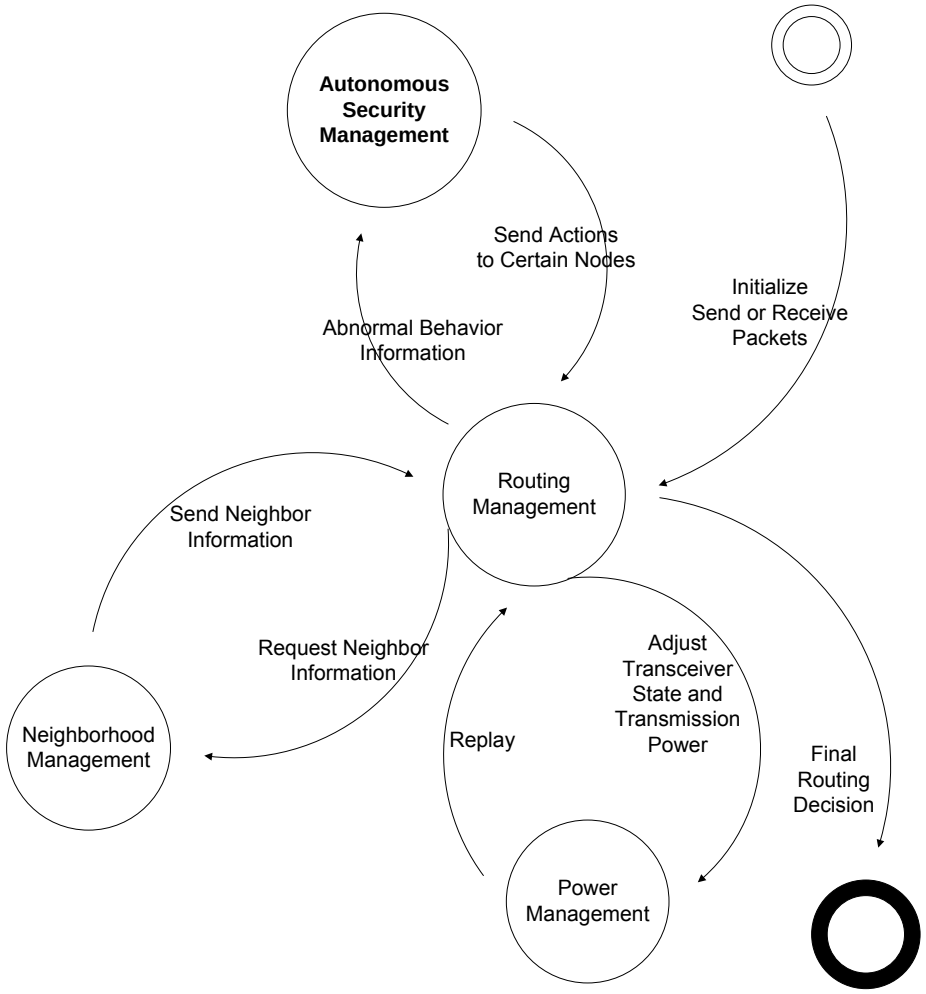


Fig 2. State Machine Diagram of BIOSARP

ISBN: 978-1-61804-039-8

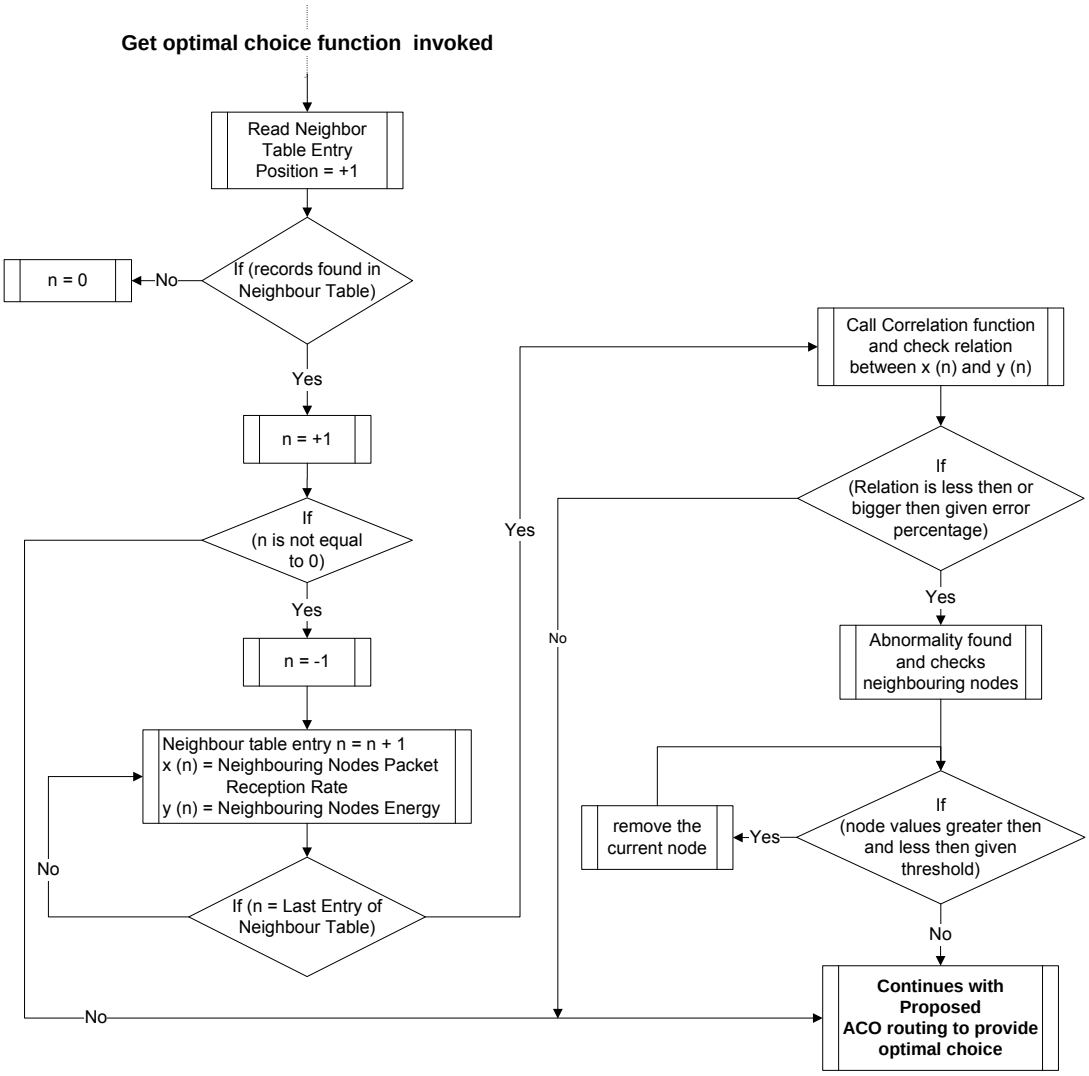


Fig 3. Flow Chart of BIOSARP Autonomous Security Management

$x, y \in \{0...255\}^N$, $N = l/8$,

$$\rho = \frac{\sum_{i=1}^{n}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i-\bar{X})^2 \sum_{i=1}^{n}(Y_i-\bar{Y})^2}} \quad [15] \quad (1)$$

If the relation is having less or equal difference according to the given error rate, the process jumps to the selection criteria. Else, if the variation goes beyond detection agent is called to thoroughly check entry-by-entry in the current neighbour table. In the inspection, if any neighbouring nodes characteristics exceed the given threshold, the particular neighbour node is categorized as non-self by the decision agent. The decision s based on the Equation 2 to classify node as self or non-self. After categorization defence agent removes the non-self marked neighbouring nodes from neighbouring table.

$$\text{match}(f,\mathcal{E},I,D) = \begin{cases} malicious, f(I,\alpha) \geq 1 - \mathcal{E} \\ benign, otherwise \end{cases} [15] \quad (2)$$

where, I = Input string, D = Decision Agent's matching String, f = Matching Function, $\mathcal{E}$ = Matching Threshold.

In security mechanism incur certain delay time period at initialization phase. To secure WSN at the initial stage, BIOSARP is additionally enhanced with human immune blood brain barrier (BBB) system which secures WSN communication even in the initialization and learning period. BBB is based on packet encryption and decryption. The encryption based security is based on work done on SRTLD [25]. In addition, BIOSARP acquire random generator function encrypted with mathematical function from [25]. The output of random generator function is used to encrypt specific header fields in the packet such as source, destination addresses and packet ID.

ISBN: 978-1-61804-039-8

4 Results and Comparisons

In the simulation study, NS-2 simulator is used to develop BIOSARP functional modules. Fig 4 shows the countermeasures against abnormalities found in WSN.

The simulation scenario is maintained as in [15]. In case of BIOSARP, it is assumed that there is no any energy consumption until the data forwarding takes place, as BIOARP is an on-demand routing protocol. After the network has suffered attack by 10 malicious nodes, the power consumption value increased. Once the AIS self-security measure starts functioning, the energy consummation starts to reduce. And as soon as the malicious nodes stop attacking, the power consumption comes to the normal situation as we observe at 500th second in Fig 5.

Fig 6 shows the performance of BIOSARP as the number of compromised node increases from 4 to 20. In Fig 6(a), the number of compromised nodes increases beyond 16, the delivery ratio starts decreasing. This is primarily due to the routing hole between the sink and source nodes 43, 31 and 37 becoming bigger. In Fig 6(b), the power consumption increases as the number of compromised nodes increases in order to overcome the routing hole problem. This is because the routing path becomes longer and transmission power becomes higher in the presence of compromised nodes.

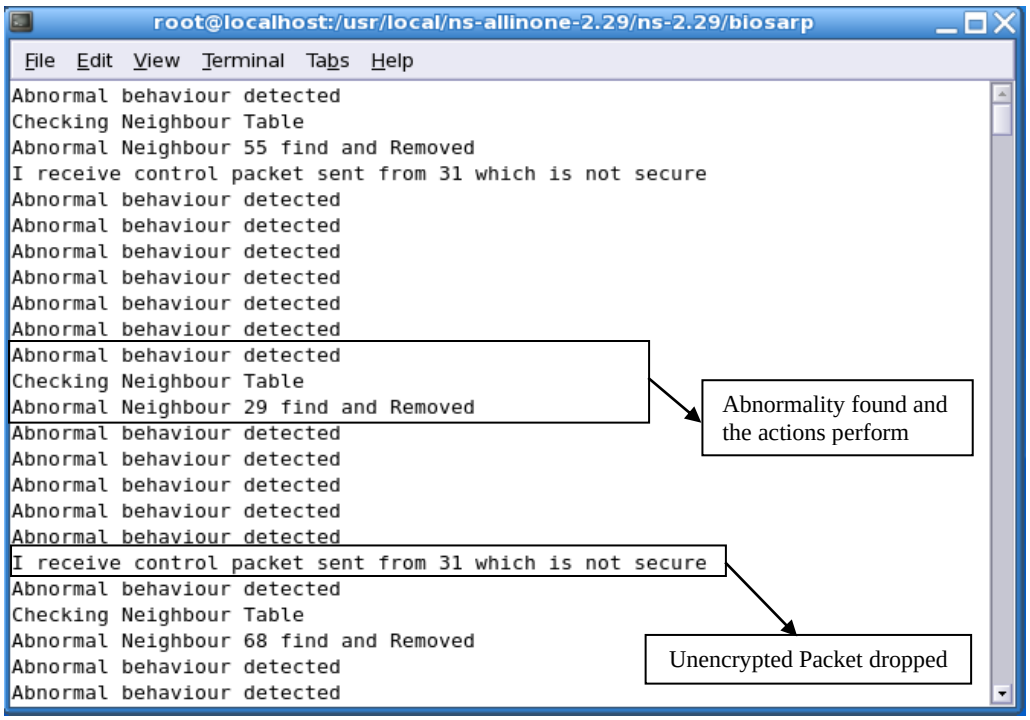


Fig 4. NS-2 showing the Abnormality and actions taken against certain nodes

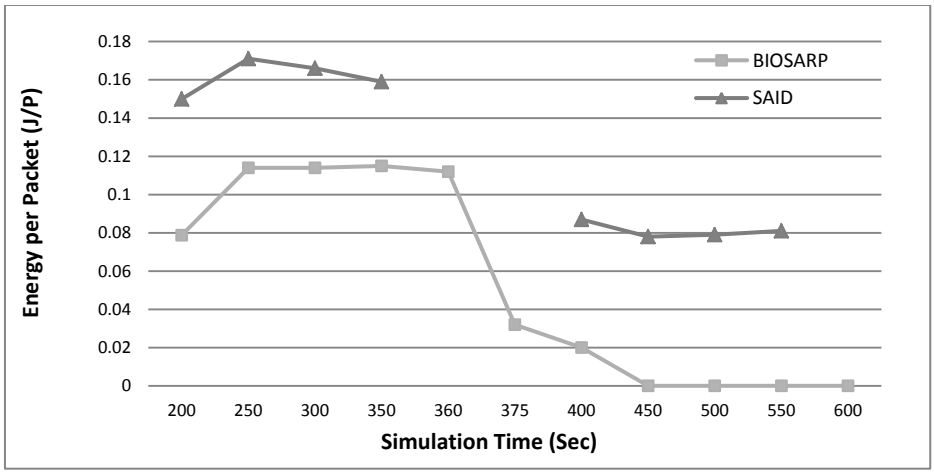
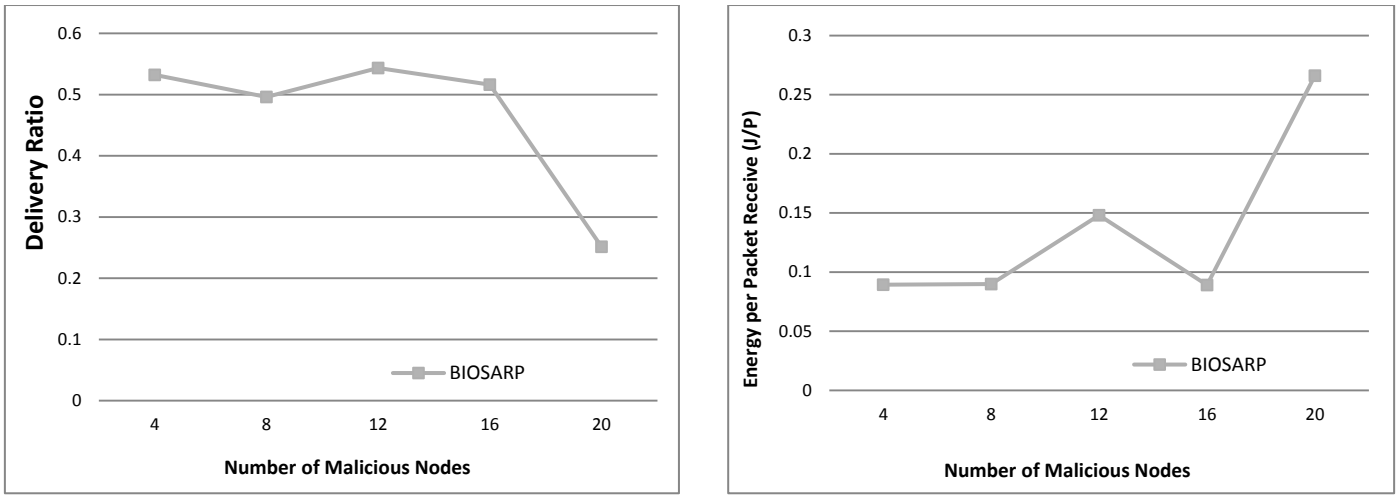


Fig 5. BIOSARP & SAID Comparison in terms of Energy



(a) (b)

Fig 6. Influence of increasing compromised nodes in network performance: a) delivery ratio and b) power consumption.

5 Conclusion and Future Work

Here, we have proposed a biological inspired self-organized secure autonomous routing protocol named as BIOSARP for WSNs. The security system is based on AIS. The proposed mechanism can successfully detect the non-self antigens (most common known attacks). We also showed that the proposed system will provide security at no additional control or energy costs to the system. Our proposal clearly demonstrates that AIS based security has the potential to offer significantly higher performance in WSN due to its significantly less control, energy and computational cost.

Our immediate future work will involve building and testing the architecture by the implementation of proposed system in the real WSN test bed.

Acknowledgment

I wish to express my sincere appreciation, sincerest gratitude to University Technology Malaysia for their support and special thanks to researchers in Telematic Research Group.

References

[1] S. Balasubramaniam, *et al.*, "Biologically Inspired Self-Governance and Self-Organisation for Autonomic Networks," presented at the Proceedings of the 1st international conference on Bio inspired models of network, information and computing systems, Cavalese, Italy, 2006.

[2] S. Balasubramaniam, *et al.*, "Towards integrating principles of Molecular Biology for Autonomic Network Management," in *Hewlett Packard university Association (HPOVUA) conference*, Nice, France., 2006.

[3] P. Boonma and J. Suzuki, "MONSOON: A Coevolutionary Multiobjective Adaptation Framework for Dynamic Wireless Sensor Networks," presented at the In Proc. of the 41st Hawaii International Conference on System Sciences (HICSS), Big Island, HI, 2008.

[4] N. Mazhar and M. Farooq, "BeeAIS: Artificial Immune System Security for Nature Inspired, MANET Routing Protocol, BeeAdHoc," *Springer-Verlag Berlin Heidelberg*, vol. LNCS 4628, pp. 370–381, 2007.

[5] G. D. Caro, *et al.*, "AntHocNet: An Ant-Based Hybrid Routing Algorithm for Mobile Ad Hoc Networks," *LNCS 3242*, pp. 461-470, December 16 2004.

[6] Z. Liu, *et al.*, "A swarm intelligence routing algorithm for manets," in *IASTED International Conference on Communications Internet and Information Technology*, St. Thomas, USA, 2004.

[7] S. Rajagopalan and C. C. Shen, "ANSI: A swarm intelligence-based unicast routing protocol for hybrid ad hoc networks," *Journal of Systems Architecture*, vol. 52, pp. 485-504, 2006.

[8] O. H. Hussein, *et al.*, "Probability Routing Algorithm for Mobile Ad Hoc Networks Resources Management," *IEEE*, vol. 23, DECEMBER 2005 2005.

[9] Hussein and T. Saadawi, "Ant routing algorithm for mobile ad-hoc networks (ARAMA)," in *IEEE conference Proceedings on: Performance, Computing, and Communications*, 2003, pp. pp. 281-290.

[10] Shuang, *et al.*, "An Ant-Based On-Demand Energy Routing Protocol for Ad Hoc Wireless Networks," in *International Conference on Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007*, 2007, pp. 1516-1519.

[11] H. F. Wedde, *et al.*, "BeeAdHoc: An Energy Efficient Routing Algorithm for Mobile Ad Hoc Networks Inspired by Bee Behavior," presented at the GECCO, Washington, DC, USA., 2005.

[12] K. Saleem, *et al.*, "Ant Colony Inspired Self-Optimized Routing Protocol based on Cross Layer Architecture for Wireless Sensor Networks," *WSEAS TRANSACTIONS on COMMUNICATIONS (WTOC)*, vol. 9, pp. 669-678, 2010.

[13] K. Saleem, *et al.*, "Ant based Self-organized Routing Protocol for Wireless Sensor Networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. Vol. 2, pp. 42-46, August 2009.

[14] K. Saleem, *et al.*, "Cross Layer based Biological Inspired Self-Organized Routing Protocol for Wireless Sensor Network," presented at the TENCON 2009, Singapore, 2009.

[15] J. Ma, *et al.*, "SAID: A Self-Adaptive Intrusion Detection System in Wireless Sensor Networks," in *Information Security Applications*, ed, 2007, pp. 60-73.

[16] G. Chen, *et al.*, "An improved ant-based routing protocol in Wireless Sensor Networks," in *Collaborative Computing: International Conference on Networking, Applications and Worksharing, 2006. CollaborateCom 2006.*, New York, NY, 2006, pp. 1-7.

[17] T. Stuetzle and M. Dorigo, "A Short Convergence Proof for a Class of ACO Algorithms," *IEEE Transactions on Evolutionary Computation*, vol. 6, pp. 358-365, 2002.

[18] M. Chen, *et al.*, "Mobile Agent Based Wireless Sensor Networks," *JOURNAL OF COMPUTERS*, vol. 1, 2006.

[19] K. Saleem, *et al.*, "A Self-Optimized Multipath Routing Protocol for Wireless Sensor Networks," *International Journal of Recent Trends in Engineering (IJRTE)*, vol. 2, 2009.

[20] A. K. Pathan, *et al.*, "Security in Wireless Sensor Networks: Issues and Challenges," in *Proceedings of 8th IEEE ICACT 2006*, Phoenix Park, Korea, 2006, pp. 1043-1048.

[21] G. Li, *et al.*, "A Distributed Intrusion Detection Scheme for Wireless Sensor Networks," in *The 28th International Conference on Distributed Computing Systems Workshops*, Beijing, China, 2008, pp. 309-314.

[22] C. H. Lim, "LEAP++: A Robust Key Establishment Scheme forWireless Sensor Networks," in *The 28th International Conference on Distributed Computing Systems Workshops*, Beijing, China, 2008.

[23] H. Wang, *et al.*, "Comparing Symmetric-key and Public-key based Security Schemes in Sensor Networks: A Case Study of User Access Control," in *The 28th International Conference on Distributed Computing Systems*, Beijing, China, 2008.

[24] K. Xing and F. Liu, "Real-time Detection of Clone Attacks in Wireless Sensor Networks," in *The 28th International Conference on Distributed Computing Systems*, Beijing, China, 2008.

[25] A. Ali and N. Fisal, "Security enhancement for real-time routing protocol in wireless sensor networks," in *5th IFIP International Conference on Wireless and Optical Communications Networks. WOCN '08.*, 2008, pp. 1-5.

[26] K. Saleem, *et al.*, "Proposed Nature Inspired Self-Organized Secure Autonomous Mechanism for WSNs," in *Asian Conference on Intelligent Information and Database Systems*, Quang Binh University, Dong Hoi City, Quang Binh Province, Vietnam, 2009, pp. 277-282.

ISBN: 978-1-61804-039-8