Proposed Nature Inspired Self-organized Secure Autonomous Mechanism for WSNs

K. Saleem¹, N. Fisal², M. S. Abdullah³, A.B. Zulkarmwan, S. Hafizah, S. Kamilah
Faculty of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Malaysia
¹kashnet@hotmail.com, ²sheila@fke.utm.my, ³msharila@citycampus.utm.my

Abstract—The field of wireless sensor network (WSN) is an important and challenging research area today. Advancements in sensor networks enable a wide range of environmental monitoring and object tracking applications. Secure routing in sensor networks is a difficult problem due to the resource limitations in WSN. Moreover, multihop routing in WSN is affected by new nodes constantly entering/leaving the system. Therefore, biologically inspired algorithms are reviewed and enhanced to tackle problems arise in WSN. Ant routing and human self security systems have shown an excellent performance for WSNs. Certain parameters like energy level, link quality, loss rate are considered while making decision. This decision will come up with the optimal route and also to take best action against the security attacks. In this paper, the design and initial work on BIOlogical-inspired self-organized Secure Autonomous Routing Protocol (BIOSARP) for WSNs is presented. The proposed bio-inspired algorithm will also meet the enhanced sensor network requirements, including energy consumption, success rate and time.

Keywords- ANT Colony, Human Immune System, Self-healing, Self-Organized, Wireless Sensor Network

I. INTRODUCTION

Wireless communication plays an important role these days in the sector of telecommunication and has huge importance for future research. This 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 very frequently available to the end-user. The fast growth makes wireless communication more and more complex. Also some of infrastructureless WSNs deployment area is out of human reach. The above mentioned challenges like growing complexity, unreachable maintenance and unsecure communication need new mechanisms. The new mechanism can maintain the features of WSNs in a complete autonomous way, such as multihop routing and dynamic environmental changes. In order to address autonomous capability for multihop WSNs, it has been visualize that self-organized network application can understand the network operational objectives. Additionally, 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 issue. The area of bio-inspired network engineering has the most well known approaches which are swarm intelligence (ANT Colony, Particle swarm), AIS and intercellular information exchange (Molecular biology)[1-4]. WSN routing algorithms based on ant colony optimization (ACO) has been presented in the last few years, such as [5], Sensor-driven Cost-aware Ant Routing (SC), the Flooded Forward Ant Routing (FF) algorithm, and the Flooded Piggybacked Ant Routing (FP) algorithm [6], Adaptive ant-based Dynamic Routing (ADR) [7], Adaptive Routing (AR) algorithm and Improved Adaptive Routing (IAR) algorithm [8], E&D ANTS [9]. The author of [4] propose misbehavior detection in nature inspired MANET protocol, BeeAdHoc. iNet proposed in [10] detects and eliminates the antigens (e.g., Viruses) from the BiSNET/e enabled networks. 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 been investigated.

This paper propose an architecture named as BIOSARP, consist of the most well known and successful approaches. ACO method is utilized for the optimum route discovery in multihop WSN. This routing algorithm will be further enriched with a self-healable security mechanism inspired by AIS. These techniques will be accomplished by assigning each procedure to the group of agents. The agents will work in a decentralized way to collect data and/or detect an event on individual nodes and carry data to required destination through multihop communication.

The next section reviews the related research for optimum route discovery through ACO and security of network routing protocol using the AIS approach. Section 3 describes the way to implement this autonomously secure routing mechanism. Section 4 shows some of the preliminary work. The conclusion and future work are stated under section 5.

II. RELATED RESEARCH

A. Overview of Ant Routing in WSN

Ant colony algorithms were first proposed by Dorigo et al [5] as a multi-agent approach to difficult combinatorial optimization problems like the traveling
salesman problem (TSP) and the quadratic assignment problem (QAP), 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 the global optima with non-zero probability in the solution space [11] and their performance have greatly matched many well-studied stochastic optimization algorithms, for example, genetic algorithm, pattern search, GPASP, and annealing simulations [5].

Sanjoy Das et al have given an on-line ACO algorithm using AntNet techniques for MSDC [12] which has been formalized to be a typically Minimum Steiner Tree problems. They also have proposed an improved algorithm by adding another type of ants, random ants, just like the newspaper deliverer, whose main task is to dissipate information gathered at the nodes among other neighboring nodes. Practically, simulation results also show that their algorithms are significantly better than address-centric routing. In these proposed algorithms the forward ants normally spend a long time. There is a bug of dead lock in their algorithms. In their improved algorithm, a large amount of random ants are needed.

Zhang et al. [6] proposed three ant-routing algorithms for sensor networks. The SC algorithm is energy efficient but suffers from a low success rate. The FF algorithm has shorter time delays; however, the algorithm creates a significant amount of traffic. Despite high success rate shown by the FP algorithm that it is not energy efficient.

ADR algorithm using a novel variation of reinforcement learning was proposed by Lu et al. [7]. The authors used a delay parameter in the queues to estimate reinforcement learning factor. In [13] proposed a novel approach for WSN routing operations. Through this approach the network life time is maintained in maximum while discovering the shortest paths from the source nodes to the base node using an evolutionary optimization technique. The research has also been implemented on microchip PIC® series hardware, called PIC12F683.

In [8] propose two adaptive routing algorithms based on ant colony algorithm, the AR algorithm and the IAR algorithm. To check the suitability of ADR algorithm in the case of sensor networks, they modified the ADR algorithm (removing the queue parameters) and used their reinforcement learning concept and named it the AR algorithm. The AR algorithm did not result in optimum solution. In IAR algorithm by adding a coefficient, the cost between the neighbor node and the destination node, they further improve the AR algorithm. [9] propose E&D ANTS based on Energy*Delay metrics for routing operations. Their main goal is to maintain network lifetime in maximum and propagation delay in minimum by using a novel variation of reinforcement learning (RL). E&D ANTS results was evaluated with AntNet and AntChain schemes.

1) **Comparison of the most recent ANT based routing in WSN:** SC and [13] depends on the energy metric while FF based on delay. IA and IAR is the modification of ADR which used a delay parameter in the queues to estimate reinforcement learning factor. In FP they combine the forward ant and data ant to enhance the success rate. E&D ANT based on energy*delay metrics for routing operations. In our proposed BIOSARP, the best values of velocity, PRR and remaining power mechanism [14] are used to select forwarding node because velocity alone does not provide the information about link quality. The best link quality usually provides low packet loss and energy efficient [15]. Another novel feature of BIOSARP is it utilizes the remaining power parameter to select the forwarding candidate node. The remaining power assists the source node or intermediate node to distribute the forwarding load to all available forwarding candidates and hence avoid the routing holes problem. BIOSARP is enhanced with any-cast forwarding scheme to route the data towards the best and nearest destination.

<table>
<thead>
<tr>
<th>Title of the Mechanism</th>
<th>Velocity or Level</th>
<th>Remaining Power</th>
<th>Link Quality</th>
<th>Types of Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SC</strong></td>
<td>Energy</td>
<td>Efficient</td>
<td>Multicast (one-to-many) and Converge-cast (many-to-one)</td>
<td></td>
</tr>
<tr>
<td><strong>FF</strong></td>
<td>Forward</td>
<td>Network</td>
<td>Multicast and Converge-cast</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent + Data</td>
<td>Layer Estimation</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FP</strong></td>
<td></td>
<td></td>
<td>Multicast and Converge-cast</td>
<td></td>
</tr>
<tr>
<td><strong>AR</strong></td>
<td>Heuristic Correction Factor</td>
<td>Broadcast, Unicast &amp; Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IAR</strong></td>
<td>Heuristic Correction Factor</td>
<td>Geographic Routing</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Okdem</strong></td>
<td>Path costing</td>
<td>Energy Level</td>
<td>Broadcast, Unicast &amp; Multicast</td>
<td></td>
</tr>
<tr>
<td><strong>E&amp;D ANTS</strong></td>
<td>Energy</td>
<td>Network Layer Estimation</td>
<td>Broadcast, Unicast &amp; Multicast</td>
<td></td>
</tr>
</tbody>
</table>

**B. Security in WSNs**

Because of resource constraint and vulnerabilities of wireless communication, it is easier to suffer all kinds of attacks, as sensor nodes are mostly deployed in the unprotected/hostile environment. 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 so on [16]. Many papers have proposed prevention countermeasures of these attacks and the majority of them are based on encryption and authentication. However, these prevention measures in WSN can reduce intrusion to some extent. In this case, intrusion detection system (IDS) can work as second secure defense of WSN to further reduce attacks and insulate attackers.

ACO is also utilized for intrusion detection in [17, 18]. The authors have introduced the concept of tabu list, where for every session the list would like to store the pheromone trace or path that is prone to attack.

In [19], the ACO based intrusion feature selection algorithm is proposed. The FDR is taken in as the heuristic information for ACO. The authors have adopted the Least Square based SVM estimation to avoid training of a large number of SVM classifier. The results have been demonstrated, by which they have show the detected attacks as probe, dos and U2R&R2L intrusions.

1) Overview of AIS based Security in WSN: In [20], the authors have proposed SAID with three-logic-layer architecture. SAID adopt the merits of local IDS and 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.

In [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, 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.

Since the characteristics of WSN (e.g. resource constrains of sensor nodes, Ad Hoc mechanism, the sensor node may be static after deployment, etc), most IDS for internet network or mobile Ad Hoc network cannot be applied in WSN well. Therefore, the researches in IDS of WSN are still at the beginning [20]. The operation of BeeHive algorithm requires an initialization phase (30 seconds) before the AIS learning could start. It is followed by the learning (50 seconds) and protection phases to respectively learn the BeeHive normal behavior and detect the routing attacks [4].

2) Overview of keying based Security in WSN: Chien-Chung Su et al proposed two approaches to improve the security of clustering-based sensor networks: authentication based intrusion prevention and energy-saving intrusion in [22]. The proposed authentication-based intrusion prevention is enhanced from μTESLA which uses one-time key chains. Therefore, each CH needs to be loosely time synchronized with its member nodes. All sensor nodes are loosely time synchronized. The synchronization in WSNs is impossible to have an accurate synchronization.

Due to the factor of initialization phase, WSN need security mechanism to be in operation before the network deployment. As stated in [23] 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 [24]. The performance of PKC based security schemes is still not well investigated due to the special hardware characteristics.

In [25] the 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 [26] the author presents the security enhancement which uses the 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. The mechanism pairwise key establishment (PKE) based on transitory master keys as discussed in [23] is particularly useful for the 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) Comparison of the most common secure routing protocols in WSN: The security measures as given above have still lot of holes and could not tackle the most common WSN routing attacks. In front of the currently running security protocols, BIOSARP will protect WSN from the most common attacks yet stated [27, 28]. Our proposed BIOSARP autonomously secure routing mechanism will use these metrics to make security decisions: link quality, energy consumption, key establishing time, memory overhead and message complexity as mentioned in Table III. Attacks and intrusions are handled by the Artificial Immune misbehavior/IDS. As further the security enhancement
based on human nerve barrier system will also helps to cut down the feedbacks. This barrier system will help to differentiate between a good and malicious node.

TABLE II. COMPARISON OF THE MOST RECENT SECURITY BASED PROTOCOLS

<table>
<thead>
<tr>
<th>Title of the Protocol</th>
<th>Tackled Attacks</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>[25] by Su</td>
<td>Bogus Routing Information, Hello Floods, Black Hole, Select Forward</td>
<td>Sensor nodes cannot move and new sensor nodes cannot be added after the pairwise keys are established</td>
</tr>
<tr>
<td>SAIID</td>
<td>Non-self antigens</td>
<td>Assumption of no attack in first 30 seconds</td>
</tr>
<tr>
<td>[21] by Li</td>
<td>Worm hole, Sybil</td>
<td>Assumption of no attack while initialization</td>
</tr>
<tr>
<td>[21] by Li</td>
<td>Fabric information attack, Select forward, Sink hole, Hello attack, Worm hole attack</td>
<td>Group based Intrusion mechanism and only internal detection</td>
</tr>
<tr>
<td>[25]</td>
<td>Clone Attacks</td>
<td>Have less overheads but tackling only kind</td>
</tr>
<tr>
<td>LEAP++</td>
<td>Clone Attacks, DoS Attacks, Worm hole attacks</td>
<td>Assuming NCC is willing invest enough time. All nodes deployed at a time are programmed to start neighbor discovery at some delay time after being airdropped.</td>
</tr>
<tr>
<td>STRLD</td>
<td>HELLO Flood, Selective Forwarding</td>
<td>Each sensor node is static and aware of its location. Sink is a trusted computing base.</td>
</tr>
</tbody>
</table>

III. METHODOLOGY

System design deals mainly with the development of state machine and flow chart diagram of the sections as routing, security and energy management for BIOSARP as shown in figure 1.

$$p_{ij}^k(t) = \frac{[r_{ij}(t)]^\alpha[n_{ij}(t)]^\beta}{\sum_{h \in I}[r_{ij}(t)]^\alpha[n_{ij}(t)]^\beta}$$ (1)

- $p_{ij}^k(t)$ overall desirability for ant $k$ located in city $i$ to choose to move to city $j$.
- $T_{ij}$ is a value stored in a pheromone table.
- $n_{ij}$ is an heuristic evaluation of edge $(i, j)$.

Our proposed self-organized system contains mainly two section based on routing and security. The routing will be totally based on ACO. Routing decision will achieved through probabilistic decision rule as shown in (1) [13] by enhancing it with our parameters given in table III. The decision will depends on our used metrics as, velocity, PRR and remaining power mechanism.

ACO will be further enhancing with an additional security through AIS algorithm. This module will be based on AIS to self-secure and self-heal the network from the foreign bodies or attacks. AIS make its decision by sensing or detecting the intrusion based on additional parameters / metrics: packet dropping rate, packet mismatch rate and packet sending power as given in table III. AIS will do the detection for intruders which will be further increased by key management system.

![System State Diagram](image)

Figure 1. System State Diagram.

Routing cycle attacks will be stopped by involving search ant agent. The structure of BIOSARP is very complex and immense; that is to tackle the attacks in maximum. The algorithm for each component in the designed system has been written and relations between the system models are established. Energy management has been evolved to maintain the energy consumption of every sensor node in WSN. Intrusion detection will be based on AIS which will make decision by using metrics as given in table III. Security mechanism will be based on three layer architecture as given in figure 2.

TABLE III. ROUTING AND SECURITY METRICS

<table>
<thead>
<tr>
<th>Tackled Attacks</th>
<th>Security Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td>Sink hole attack [21], Select forward, Black hole [21]</td>
</tr>
<tr>
<td>Node 2</td>
<td>Message alter attack [21], Hello attack, Worm hole [21, 25]</td>
</tr>
<tr>
<td>Node n</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring will be performed depending on the parameters as given in table III. If there is any abnormality found it will generate decision agent. When the intruder alarm will be generated by the monitoring agents, the security management will implements authentication.
IV. PRELIMINARY WORK

To evaluate the above analysis, we use network simulator 2 (NS2) to construct the network topology as given in figure 3. The topology is described as a randomly deployed 12-node sensor network. The program is written in NesC programming language to implement the biological inspired routing algorithm.

In figure 3, each link is bidirectional and the weighting value of the link depends on the power consumption (nJ/bit) and ant’s moving time delay (ms). After the source nodes produce a quantity of artificial ants or packets conforming to the Poisson distribution, the destination nodes are randomly chosen by average probability. When one packet passes through a node by a certain speed, the node takes the first step to gather all the ant agents into buffer storage and then selects the optimal path from its routing table to transfer packets. In this way all the ants disperse in as many paths as possible to achieve the balance of the load. A fixed size of one packet is considered in our simulation. The experimental parameters used to configure the system according to WSN are listed in Table IV.

Initial result through this implementation is the pheromone table on each node. As an example pheromone table at node 0 is shown in table V. The pheromone table at each node contains the pheromone value for the next node towards the required destination. While the network is online, the routing table is directly built up through pheromone table exponential transformation.

V. CONCLUSION AND FUTURE WORK

Here, we have proposed a biological inspired secure autonomous routing mechanism named as BIOSARP for WSNs. The routing decision will be based on ACO and the self-security on AIS. These decisions will be dependent on our use metrics. The proposed mechanism will successfully detect the non-self antigens (most common known attacks). We also find that 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. The efficient utilization of these resources is a key challenge in WSNs. While enhancing we will also improve this AIS principle by adopting a special feature away. Simulation methods for the AntNet were attempted in [30] where the parameters \((c, a, a', e, h, t)\) were set to \((2, 10, 9, 0.25, 0.04, 0.5)\).
from human nerve structure called as barrier system. This would be a cardinal step in deploying BIOSARP in real world WSNs.

Our immediate future work will involve building and testing the architecture by the direct implementation of ACS and AIS as described in this paper. Onwards, other ant colony variants such as negative reinforcement, MaxMin Ant System will also be considered. The integrated algorithm of AIS will be also enhanced by adding more features by nature.

ACKNOWLEDGMENT

I wish to express my sincere appreciation, sincerest gratitude to Ministry of Higher Education Malaysia for their full support and Research Management Center, Universiti Teknologi Malaysia (UTM) for their partial and special thanks to researchers in Telematic Research Group, UTM.

REFERENCES


