I J C T A, 9(2) 2016, pp. 997-1006

AN EFFICIENT ANT COLONY OPTIMIZATION PROTOCOL FOR SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

[1]V. Tharinie and [2]Pandiyaraj

ABSTRACT

Optimal path selection is a challenging task in Wireless Sensor Networks (WSNs). To obtain various objectives in WSNs, efficient routing protocols are designed to satisfy the requirements. Certain limitation such security threats and lower data rates are encountered. This work, proposed an adaptive secure routing protocol owing with the bio inspired mechanisms. To achieve route security, two optimal paths have been selected using distributed ant-based methodology. Initially, ants are deployed in a network and each ant listened to packets. On receiving a packet, it will check whether it is the destination. If it is, it will reply on the path reserved to reach the source or it will forward to next node. This process is repeated until the destination is reached. In the path, set of ant nodes is involved during data transmission. The energy of these ants will fall radiantly. If an ant fails, the path will be broken. In order to improve the performance of network, Ant Colony Optimization (ACO) is proposed. During the deployment of network, a colony will be established in a region. A colony comprises of an ant head and set of nodes. When an ant sends a packet it will transmitted to ant head and it will forward to all ant heads until the destination is reached. Then the ant will communicate using ant head to transfer data to destination. Simulation results show that proposed routing protocol can perform better in many scenarios.

Index terms: Wireless Sensor Networks, optimal path, routing, data transmission, Ant Colony Optimization, security.

1. INTRODUCTION

Deployment of WSNs is usually on areas where wireless or wired networks are not viable to be configured or established. For the purpose of environmental monitoring, WSNs with high power sink and low power sensor nodes are used. WSN usually operates on a distributed or a decentralized manner, in which it has a self-configuring and self-healing capacity. WSN is more susceptible to various types of security attacks, since it owes multihop distributed architecture and a physical antagonistic environment. Due to the media access, physical nature of network layer, attackers can by far launch an attack in the WSNs. Attaining higher security is the main goal for the deployment and designing of the sensor architecture. Since, WSN is organized in a ruthless and intense environment; it does not provide security by physical monitoring of the attacks.

Security consideration has an impact with the applications of monitoring and military based applications in WSNs. The nodes in WSN are of low cost and small in its size, thus it lags in providing heavy security protection against attacks. Demanding resources like higher memory, more battery and processing power with increased cost, provides higher security mechanisms against attacks. Owing to not providing a tampering resistance, false data can be injected in the source to destination path, sensitive data may be extracted from the route and re-configuring of nodes can also be done by the attackers.

[1] Research scholar, Master of Technology, Computer Science and Engineering, SRM University, Ramapuram Campus, Chennai, *E-mail: tharinieschola2016@gmail.com*

[2] Assistant Professor, Computer Science and Engineering, SRM University, Ramapuram Campus, Chennai.

Developing a secure routing algorithm exploits an optimal solution to countermeasure the security attacks towards the network layer. While transmitting a data from source to destination with muti-hop techniques, the data is susceptible towards various security attacks. Secure routing algorithms also provide desirable protection to such kind of networks.

An attacker can conduct variety of security attacks against WSN, such as blackhole, greyhole, sinkhole, false routing updates, packet modification attack, packet misdirecting attack, and hello flood attack [2, 3 Malfunctioning of routing while transmitting the data from source to destination causes a viable impact on attacks. Some of the routing attacks have higher severity and some may have lower severity. For instance, in some cases sinkhole attack and blackhole attack drop the packets and causes DoS (Denial of Service attacks), whereas in greyhole attack, selected packets can be forwarded to next hop. These network layer security attacks can be prevented by appropriate secure routing protocol.

To deploy and design a multihop wireless sensor networks, security routing is an important factor. AS compared to single hop wireless networks, multi hop wireless networks shows higher susceptibility to provide security towards attacks. The reason behind selecting a multihop a network is that it provides no centralized and distributed architecture. Designing an appropriate secure routing protocol for WSN is a challenging task. The routing protocol should meet certain constraints such as route discovery, routing overheads and data delivery in a WSNs. Secured routing protocol has been designed and formulated by the researchers. Some of the important approaches are multipath mechanisms, bioinspired mechanisms and cross-layered mechanisms.

To encounter the optimal path, to transmit the data from source to destination certain parameters can be exchanged between the layers of the protocol [4]. Hence, it requires higher memory, battery resources and more computation for cross-layer mechanisms. The main advantage in cross-layer mechanism is that it provides multilayer security threats. In multipath mechanism, two or more paths are established from source to destination [5,6]. Multiple route are known to transmit the data instead of one path, hence it shows fault tolerant compared to that of the single path. Bioinspired mechanisms are considered more robust as they provide interesting solution for routing due to their inherent scalable features [7].

In this paper, extend optimal path detection and focused on providing an efficient secure data communication for ANT network. Here, a colony established by grouping the ants and the ants are managed by an ant header. The ant head is chosen by choosing the ant with maximum energy. The ant head is responsible for communications between colonies. When an ant sends a packet, the ant head of that ant's colony will receive it. It will forward to all ant heads. If the destination is found the respective ant head will reply back and then the ant will communicate using the path through ant heads. By communicating through the ant heads the number of ants involved in a path is reduced exponentially compared to existing methods. Thus it reduces energy consumption of ants and improves network performance and life time. Rest of the paper organized as follows: section 2 presents the related work bio inspired based path selection, section 3 discusses the proposed methodology, section 4 defines the experimental results and security analysis, and section 5 concludes the paper.

2. RELATED WORK

WSNs have many real-life applications such as military applications, healthcare applications, forest and habitat monitoring, fire, heat, and pressure monitoring in a given area [8]. The major task in WSN is to select the data packets and deliver it to the destination from source. Many routing protocols are formulated by researchers so far [9][10]. Those routing protocols mainly concentrate on application nevertheless in security consideration. Security is a main concern and captures the attention, thereby more secure mechanisms are proposed by the researchers for WSN [11][12]. The security mechanism concentrates on different layers to countermeasure the risk of the situation. Secure routing mechanism is more appropriate for security attacks in network layers. In last few years, variety of secure routing protocols is proposed for sensor networks [13, 14]

The base station of the wireless sensor networks periodically broadcasts the decided routing information. The data can be easily modified, misdirected or dropped during the process of transmission. . A security mechanism termed as ìTesla [15] is proposed to neglect the data being modified during the broadcast of information from the BS. The authenticated broadcast is performed by the ìTesla using the symmetric cryptography. Due the one way hash function, this process is more expensive. An authenticated routing message in sensor network (ARMS) [16] is formulated to overcome the backlogs encountered in ì Tesla. ARMS uses short one way hash chain and shared secret key. Enhancement of fault tolerant ad hoc on-demand distance vector (ENFAT-AODV) [17] has been proposed to address the node failure. When a node failure is occurred in the decided route, back path is established to overcome the node failure. Since the sensor nodes are in distributed manner, the deployment of neighbor selection becomes an important task. Cross-layer secure routing protocol using energy harvesting mechanism in wireless sensor networks is proposed in [18]. Secure alternate path routing in sensor network (SeRINS) uses neighbor report system for the key management. This method supports in preventing attacks such as bogus routing or packet modification in WSN. Another secure approach that uses secret key cryptography with rekeying support is proposed for WSN.

The resource constraints such as computation, memory, data rates, battery power are highly desirable for the designing the WSN architecture. The security mechanisms are proposed to deploy the routing protocols to achieve long-time operations and to reserve the critical resources. For sharing of secret key and management more resources are required. For providing security Bioinspired mechanism offers fast, inexpensive and robust solutions in WSN. Ant colony optimization (ACO) is one of the bioinspired techniques, which provides robust and interesting solutions for WSN routing protocols.

Termite algorithm is inspired from the termite colonies [20]. Termite is a hybrid routing protocol to invoke routes on demand, the quality of paths are maintained in a pro-active manner by the ants. Here in the approach, backward ants uses either the same path or not, while the forward path follow randomly in a unicast directions. Optimized termite [21] has been proposed to enhance the load balancing technique. The algorithm selects the less traffic route for transmission.

Ant-dymo [22] has been proposed mainly for ad hoc networks and it concerns with the ACO. Ant-dyno, aims to reduce the packet loss and to decrement the end to end delay. The algorithm possesses two types of algorithm namely artificial ants and explorer ants. The route is exploited in a proactive manner and search for path, when no specific route is available in the routing table respectively. AntHocNet [23] uses proactive forward ants to test the quality of the available paths and exploit a new path and forward ants to discover the routes between the source and the destination. AntOR [24] has been developed to provide modification with the AntHoc routing algorithm owing with the Ant colony optimization. AntOR achieves load balancing by meeting the requirements to attain quality of service. By imposing restriction on routing information, lower control overhead can be attained.

GrAnt [25] has been proposed to satisfy the routing overhead and attains greater packet delivery based on prediction routing algorithm. GrAnt depends on both local information and global information. In [26], an ant based routing protocol with mathematical computation of bioinspired has been presented for WSN. An energy efficient ant-colonization-based routing algorithm is proposed in [27]. The packets are treated as ant, in which the communication is performed with the pheromone. Pheromone tables are maintained by the sensor node. Biologically inspired optimization for sensor lifetime (Bio4sel) [28] is distributed, autonomic and decentralized ant based routing algorithm that achieves increased network lifetime. Another energy efficient routing protocol is presented in [29]. Dynamic route identification is implemented by this approach to meet path failure caused due to intrusion or dead node. Energy efficiency and path reliability can be achieved by this approach.

To select an optimal path, an efficient bioinspired routing protocol with optimization technique has been employed. With contract, to attain memory usage, computation and battery power ACO-based routing

protocol are used since it is less expensive. Owing to the lack of security mechanisms, this technique lags in security attacks. WSN are ruthless and hostile for deployment, hence added to bioinspired mechanism certain security mechanisms should be employed.

3. PROPOSED METHODOLOGY

This section defines the optimal path routing for transmit the data to destination in ant WSN. The energy of each ant is optimized by ACO is discussed in given below section.

3.1. System overview

In this system, a colony is established by grouping the ants and the ants are managed by an ant header. The ant head is chosen by choosing the ant with maximum energy. The ant head is responsible for communications between colonies. When an ant sends a packet, the ant head of that ant's colony will receive it. It will forward to all ant heads. If the destination is found the respective ant head will reply back and then the ant will communicate using the path through ant heads.

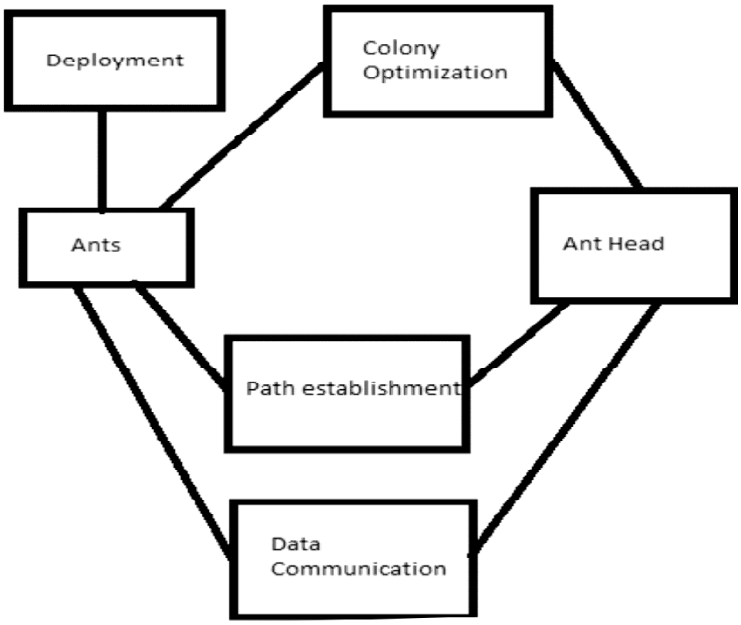

Figure 1: Overall architecture of proposed system

3.2. Network module

An undirected graph G (V, E) where the set of vertices V represent the mobile nodes in the network and E represents set of edges in the graph which represents the physical or logical links between the mobile nodes. the nodes are placed at the identical level. The nodes in the network are connected using edges in the graph, in which communication performed directly between each other. Let N denote a network of m mobile nodes, N_1, N_2...N_m distributed across the network. The pair of mobile nodes given by N_i and N_j, let tij denote the delay of transmitting a data item of unit-size between these two nodes. A mobile sink is deployed to collect data from each sensor.

3.3. Ant Colony

Consider a homogeneous WSN with a huge amount of wireless sensor nodes and a prefixed BS possessing higher functionality and capabilities. Assume, that the base station is reliable always, i.e. trusted authority (TA). Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be

interrupted from attacks on wireless channel. In Ant Colony, sensor nodes are grouped into clusters, and each colony has a Ant Head sensor node, which is elected autonomously. Leaf sensor nodes join a cluster depending on the receiving signal strength and transmit the sensed data to the destination via heads to save energy. In addition, we assume that all sensor nodes are time synchronized with symmetric radio channels, randomly distributed nodes and with limited energy. In Ant Colony network, the energy of the sensor nodes are consumed while data sensing, processing and transmission. Thus, the method that the intermediate node aggregates data and sends it to the destination is preferred than the method that each sensor node directly sends data to the destination. Based on the time division multiple access (TDMA), a sensor node moves to sleep mode to save energy when transmission or reception is not under progress.

3.4. Path Reinforcement

When an ant sends a packet, the ant head of that ant's colony will receive it. It will forward to all ant heads. If the destination is found the respective ant head will reply back and then the ant will communicate using the path through ant heads. By communicating through the ant heads the number of ants involved in a path is reduced exponentially compared to previous work.

3.5. Performance evaluation

We have conducted extensive simulations to validate the proposed algorithms. In the simulations, we assume that a bunch of sensor nodes is uniformly deployed in the sensing field. For covering the uncovered node using relay node for sink in both small and large networks, compare the relative network lifetime and security of the proposed with the data-gathering schemes, and illustrate the data-gathering algorithm with mobile sink in a randomly generated network.

4. RESULTS AND DISCUSSION

With the ant-based secure routing protocol, the performance of the WSN has been simulated realistically with the available scenarios. The simulation is conducted with the NS2 simulator using 100 nodes. The random deployment of nodes was undergone with 100 by 100 meters. The node energy is placed with 6mJ initially. The distance between the nodes does not exceed 20 meters. The individual data packet is 200 bytes. We compared proposed routing mechanism with Time-Dependent Shortest Path (TDSP) [30]. The Fig. 2 shows the simulation of cluster formation.

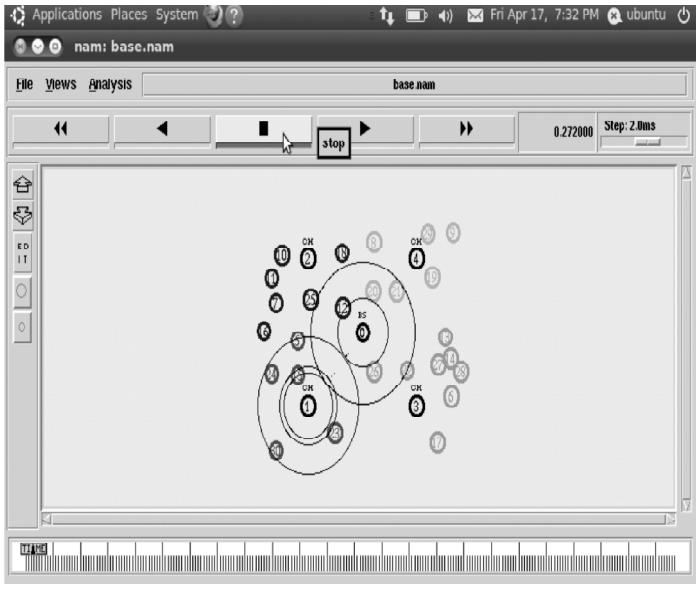

Figure 2: Simulation for cluster formation

Fig. 3 shows the network lifetime comparison of proposed ACO and existing TDSP. Initially, the performance of ACO is better than the other; however, as long as the number of nodes increases, TDSP shows performance degradation. The proposed protocol projects the performance consistently, with the variation in node densities.

Figure 3: Network lifetime comparison

Fig. 4 shows the comparison results of the overhead comparison between ACO and existing TDSP. ACO and TDSP have a relatively close network overhead as the network size increases, which indicates that both TDSP and ACO are suitable for large-scale clustered WSNs. However, by comprehensively analyzing the results in Fig.4, ACO is more suitable for large-scale clustered WSNs with a large size of clusters, thus outperforming TDSP.

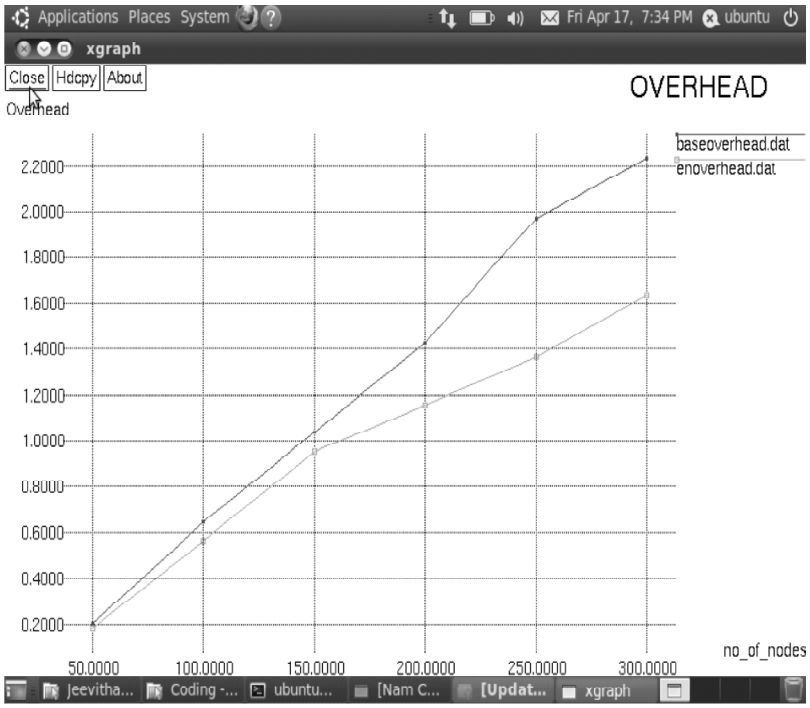

Figure 4: Overhead comparison

Fig. 5. shows that the below graph is plotted across the number of nodes and the Packet Delivery Ratio (PDR). Normally the value of PDR will get increased when compared with the existing methods. In this graph, it shows that the packet delivery ratio increased for the proposed ACO protocol model since it stores, the best individuals in the memory when compared to the existing TDSP.

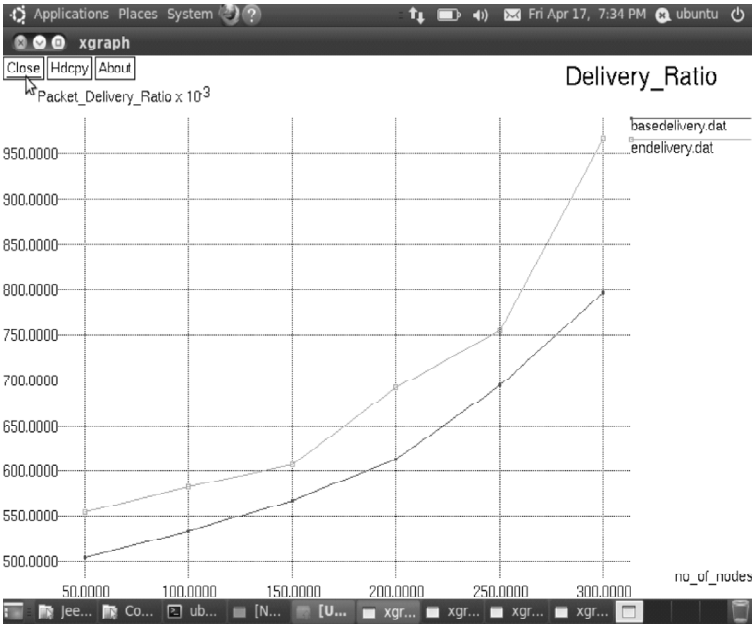

Figure 5: PDR comparison

Throughput Evaluation

Throughput is defined as the total number of packets delivered over the total simulation time. Mathematically, it can be defined as:

$$\text{Throughput} = N/1000 \quad (1)$$

Where *N* is the number of bits received successfully by all destinations.

Fig. 6 shows the throughput comparison of the proposed ACO protocol approach and the existing TDSP. It is noted that the proposed ACO protocol attains higher throughput when compared with the

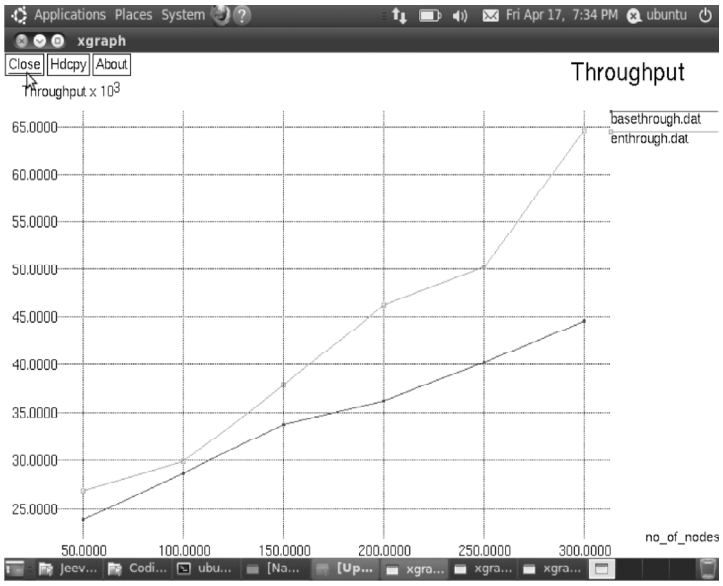

Figure 6: Throughput comparison

existing TDSP protocol. The reason is that, the probability to meet the desired event data in a short hop count is very high in such a way.

Energy Efficiency Comparison

Energy efficiency is defined to be the ratio of the amount of energy consumed per successfully packet delivered in network. Fig 7 shows that the proposed and existing comparison results with its respective energy consumption. From the figure it is obvious that the proposed ACO is consumes less energy than the existing system TDSP. When the time increases the energy consumption of the proposed system is decreases than the existing system.

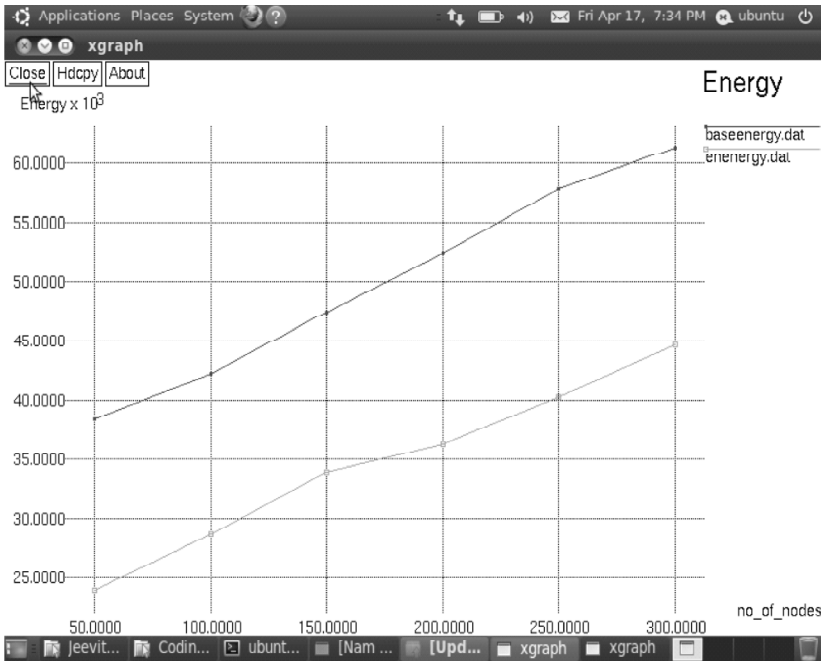

Figure 7: Energy Efficiency Comparison

5. CONCLUSION

In this paper, the issues concerned with data transmission and security has been reviewed in ANT WSNs. The deficiency of transmitting secure data using symmetric key management has been thrashed out. . We then presented ANT Colony Optimization (ACO) protocols, respectively, for Ant WSNs. In the evaluation section, we provided feasibility of the proposed Colony optimization impact on ordinary ANT network. ANT Colony is efficient in communication and solved the orphan node problem by symmetric key management in the secured transmission protocol. Lastly, the comparison in the calculation and simulation results show that the proposed protocols have better performance than existing secure protocols for WSNs. With respect to both computation and communication costs, we pointed out the merits that using ANT Colony with minimized security overhead have a preference to transmit secured data.

REFERENCES

[1] N. Alrajeh, S. Khan, J. Lloret, and J. Loo, "Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks," *International Journal of Distributed Sensor Networks.* Vol. 2013. Article ID 374796. 11 pages, 2013.

[2] N. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a Review," *International Journal of Distributed Sensor Networks.* Vol. 2013. Article ID 167575. 7 pages, 2013.

[3] S. Khan, N. A. Alrajeh, and K.-K. Loo, "Secure route selection in wireless mesh networks," *Computer Networks.* Vol. 56. No. 2. pp. 491–503, 2012.

[4] S. Khan and K. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybridwireless mesh networks," *Wireless Personal Communications.* Vol. 62. No. 1. pp. 201–214, 2012.

[5] N. Meghanathan, "A survey on the communication protocols and security in cognitive radio networks," *International Journal of Communication Networks and Information Security.* Vol. 5. No. 1. pp. 19–38, 2013.

[6] M. Radi, B. Dezfouli, K. A. Bakar, and M. Lee, "Multipath routing in wireless sensor networks: survey and research challenges," *Sensors*. Vol. 12. No. 1. pp. 650–685, 2012.

[7] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, and R. A. Rashid, "Ant based self-organized routing protocol for wireless sensor networks," *International Journal of Communication Networks and Information Security.* Vol. 1. No. 2. pp. 42–46, 2009.

[8] M. Frederickson, A Publication of the National Electronics Manufacturing Center of Excellence, 2005.

[9] M. Popescu, G. I. Tudorache, B. Peng, and A. H. Kemp, "Surveying position based routing protocols for wireless sensor and Ad-hoc networks," *International Journal of Communication Networks and Information Security.* Vol. 4. No. 1. pp. 41–67, 2012.

[10] O. Fdili, Y. Fakhri, and D. Aboutajdine, "Impact of queue buffer size awareness on single and multi service real-time routing protocols for WSNs," *International Journal of Communication Networks and Information Security.* Vol. 4. pp. 104–111, 2012.

[11] Kellner, O. Alfandi, and D. Hogrefe, "A survey on measures for secure routing in wireless sensor networks," *International Journal of Sensor Networks and Data Communications.* Vol. 1. pp. 1–17, 2012.

[12] M. Azeem, K. Khan, and A. Pramod, "Security architecture framework and secure routing protocols in wireless sensor networks-survey," *International Journal of Computer Science & Engineering Survey.* Vol. 2. pp. 189–204, 2011.

[13] Samundiswary, D. Sathian, and P. Dananjayan, "Secured greedy perimeter stateless routing for wireless sensor networks," *International Journal of Ad Hoc, Sensor & Ubiquitous Computing.* Vol. 1. pp. 9–20. 2010.

[14] G. Kumar, I. Titusb, and S. I. Thekkekarab, "A comprehensive overview on application of trust and reputation in wireless sensor network," *Procedia Engineering.* Vol. 38. pp. 2903–2912, 2012.

[15] D. Khurana and M. Singla, "Secure and authenticated source routing in wireless networks," *International Journal of Computer Science*. Vol. 12. No. 3. 2012.

[16] Z. Che-Aron, W. F. M. Al-Khateeb, and F. Anwar, "ENFAT-AODV: the fault-tolerant routing protocol for high failure rate wireless sensor networks.' in Proceedings of the 2nd International Conference on Future Computer and Communication (ICFCC '10), pp. V1467–V1471, 2010.

[17] S. Khan, K.-K. Loo, and Z. U. Din, "Framework for intrusion detection in IEEE 802.11 Wireless Mesh Networks," *International Arab Journal of Information Technology.* Vol. 7. No. 4. pp. 435–440, 2010.

[18] S.-B. Lee and Y.-H. Choi, "A secure alternate path routing in sensor networks," *Computer Communications.* Vol. 30. No. 1. pp. 153–165, 2006.

[19] V. Thiruppathy Kesavan and S. Radhakrishnan, "Multiple secret keys based security for wireless sensor networks," *International Journal of Communication Networks and Information Security.* Vol. 4. No. 1. pp. 68–76, 2012.

[20] M. S. Lin, J. S. Leu, W. C. Yu, and K. H. Li, "TBRA: termite based routing algorithm in 3D wireless sensor networks.' in Proceedings of the IEEE 75th Vehicular Technology Conference, pp. 1–5, 2012.

[21] P. G. Hoolimath, M. Kiran, and G. R. Mohana Reddy, "Optimized tERMITE: a bio-inspired routing algorithm for MANET's.' in International Conference on Signal Processing and Communications (SPCOM '12), 2012.

[22] J. A. P. Martins, S. L. O. B. Correia, and J. C. Júnior, "Ant-DYMO: a bio-inspired algorithm for MANETS.' in Proceedings of the 17th International Conference on Telecommunications (ICT '10), pp. 748–754, April 2010.

[23] G. A. Di Caro, F. Ducatelle, and L. M. Gambardella, "AntHocNet: an ant-based hybrid routing algorithm for mobile ad hoc networks," in Proceedings of the Parallel Problem Solving from Nature (PPSN '04). Vol. 3242 of Lecture Notes in Computer Science, pp. 461–470, Springer, 2004.

[24] L. J. G. Villalba, D. R. Cañas, and A. L. S. Orozco, "Bio-inspired routing protocol for mobile ad hoc networks," IET Communications. Vol. 4. No. 18. pp. 2187–2195, 2010.

[25] A. Cristina, B. Kochem Vendramin, Munaretto, M. Regattieri Delgado, and A. Carneiro Viana, "A Greedy Ant Colony Optimization for routing in delay tolerant networks," in GLOBECOM Workshops Computing and Processing, pp. 1127–1132, December 2011.

[26] S. S. Iyengar, H.-C. Wu, N. Balakrishnan, and S.Y. Chang, "Biologically inspired cooperative routing for wireless mobile sensor networks," *IEEE System Journal*. Vol. 1. No. 1. pp. 29–37, 2007.

[27] V. Mahadevan and F. Chiang, "iACO: a bio inspired power efficient routing scheme for sensor networks," *International Journal of Computer Theory and Engineering.* No. 6. pp. 1793–8201, 2010.

[28] L. B. Ribeiro and M. F. De Castro, "BiO4SeL: a bio-inspired routing algorithm for sensor network lifetime optimization.' in Proceedings of the 17th International Conference on Telecommunications (ICT '10), pp. 728–734, April 2010.

[29] N. Chauhan, A. Nain, and D. Srivastava, "A bio-inspired energy efficient routing approach to resolve broken link problem in WSN," *International Journal of Computer Applications.* Vol. 48. No. 25. pp. 18–24, 2012.

[30] Shouwen Lai, Binoy Ravindran, "Least-Latency Routing over Time-Dependent Wireless Sensor Networks", *IEEE Transactions on Computers.* Vol. 62. No. 5. 2013.