www.s2is.org
International Journal on Smart Sensing and Intelligent Systems
ISSN 1178-5608

EVALUATION OF HYBRID TRUST MODELS USING ANT COLONY OPTIMIZATION IN WIRELESS SENSOR NETWORKS

G. Edwin Prem Kumar[1], K. Baskaran[2], R. Elijah Blessing[3] and M. Lydia[4]
[1]Dept. of Computer Sciences Technology, Karunya University, Coimbatore, India
[2]Dept. of Electrical & Electronics Engg., Government College Technology, Coimbatore, India
[3]Dept. of Computer Sciences Technology, Karunya University, Coimbatore, India
[4]Dept. of Electrical Technology, Karunya University, Coimbatore, India
Email: edwinpremkumar@gmail.com

Submitted: June 2, 2016 Accepted: July 12, 2016 Published: Sep. 1, 2016

*Abstract- **Wireless sensor networks (WSNs) are prone to various kinds of threats and are subjected to several constraints like energy, communication overhead and lifetime. Application of bio-inspired algorithms based trust models has shown significant improvement in the security mechanism of the wireless sensor networks. This paper presents a brief survey on application of Ant Colony Optimization (ACO) and significance of trust models in WSNs. ACO application in routing, increase in lifetime, energy efficiency, intrusion detection and security has been presented. The performance of three hybrid trust models is evaluated based on the path length, trust calculation and energy consumption using ACO.***

Index terms*: *Ant Colony Optimization, Bad mouthing, Entropy, Fuzzy Trust, Sybil Attack.

I. INTRODUCTION

A wireless sensor network is a collection of sensing nodes, which are inexpensive and are capable of measuring, computing and communicating of information. They usually measure or sense the local environmental or other parameters, communicate the same to the neighboring nodes. These wireless sensor networks find widespread applications in military, environmental, health, home and industrial applications. The challenges faced by wireless sensor networks include limited functional capabilities, power factors, node costs, environmental factors, topology management etc. [1]. The various research issues involved in different applications of wireless sensor networks have been discussed by Kumar et al [2].

The emerging importance of WSN will continue to improve only if the inherent security threats are properly addressed. The nodes in a WSN generally have limited memory, computational power, bandwidth and battery. Hence it is necessary that the WSNs are made robust and reliable since their deployment in any environment. Techniques based on cryptography like key management schemes etc. can ensure security in communication channels in a WSN. Apart from these, recent research has shown that introduction of trust management can go a long way in securing the operation of a WSN.

Bio-inspired computing based intelligent optimization has revolutionized wireless sensor networks. A comprehensive discussion on intelligent optimization of WSN has been presented by Jabbar et al in [3]. Adnan et al. have presented a detailed survey on all the bio-mimic optimization strategies in WSNs [4]. In this paper, the impact of application of ACO in WSN has been thoroughly studied and explored. A dense static WSN comprising of 100 nodes has been assumed. It is also assumed that every node knows only its neighboring nodes depending on the wireless range. The trust value of nodes is initialized in three different ways. It is then constantly being updated by the ACO algorithm for the shortest path to be evaluated.

II. ANT COLONY OPTIMIZATION

The ant colony optimization algorithm tries to simulate the way ants behave. Ants usually tend to take the shortest path to a particular destination. As they travel they leave behind a chemical called pheromone and follow the pheromone previously deposited by other ants [5]. The pheromone quantity in the shortest path is generally the highest. Here a parallel can be drawn to the concept of trust in WSN [6]. A data packet can be safely routed in a WSN through a path with maximum trust value. The ACO algorithm is detailed in the next section.

a. ACO ALGORITHM

The Ant System is the first ACO algorithm proposed in literature [7]. Each ant generates a complete tour by choosing the various nodes according to a probabilistic state transition rule [5]. The probability with which ant *k* in sensor *r*, chooses to move to sensor *s* is given by (1) and is the ACS state transition rule.

$$s = \begin{cases} \arg\ \max_{u \in J_k(r)} \left\{ [\tau(r,u)][\eta(r,u)]^{\beta} \right\} \\ \qquad if\ q \le q_0 \\ S, \qquad otherwise \end{cases} \tag{1}$$

Where q is a random number uniformly distributed in [0…1], q_0 is a parameter ($0 \le q_0 \le 1$), and S is a random variable selected according to the probability distribution in (2), τ is the pheromone, $\eta=1/\delta$ is the inverse of the distance $\delta(r,s)$, $J_k(r)$ is the set of nodes that are yet to visited by ant *k*, now positioned on node *r* and β is the parameter which determines the relative importance of pheromone versus distance ($\beta > 0$).

$$p_k(r,s) = \begin{cases} \dfrac{[\tau(r,s)].[\eta(r,s)]^{\beta}}{\sum\limits_{u \in J_k(r)} [\tau(r,u)].[\eta(r,u)]^{\beta}} & if\ s \in J_k(r) \\ 0, & otherwise \end{cases} \tag{2}$$

The state transition rule that results from (1) and (2) is called pseudo random proportional rule and favours transitions toward nodes connected by shorter edges and a larger pheromone [5]. The global updating is done after every ant has completed its tour. The globally best ant deposits the pheromone. The pheromone level is updated by applying the global updating rule given in (3).

$$\begin{aligned} &\tau(r,s) \leftarrow (1-\alpha).\tau(r,s) + \alpha.\Delta\tau(r,s) \\ &where \\ &\Delta\tau(r,s) = \begin{cases} (L_{gb})^{-1}, if\ (r,s) \in global-best-tour \\ 0, \qquad otherwise \end{cases} \end{aligned} \tag{3}$$

Where α is the pheromone decay parameter and L_{gb} is the length of the globally best tour from the beginning of the trial.

In the process of finding the solution, when an ant visits a particular edge, the pheromone level changes according to the local updating rule, which given by (4).

$$\tau(r,s) \leftarrow (1-\rho).\tau(r,s) + \rho.\Delta\tau(r,s) \qquad (4)$$

where 0 < r <1 is a parameter and Δτ is taken as the initial pheromone level.

The local updating rule aids in shuffling of tours and enables the ants to use the pheromone information better.

III. ACO AND WSN

ACO is inspired by the behavior of ants. It has been formalized into a metaheuristic for combinatorial optimization problems [3]. For a WSN, which has the constraints of energy, memory and computational power, the heuristic algorithm can be customized to find the optimal values. The impact of ant colony based optimization in improving the performance of WSN routing, security, lifetime and energy efficiency is tremendous. A brief survey on how ACO has influenced WSN is presented in this section (Fig. 1).

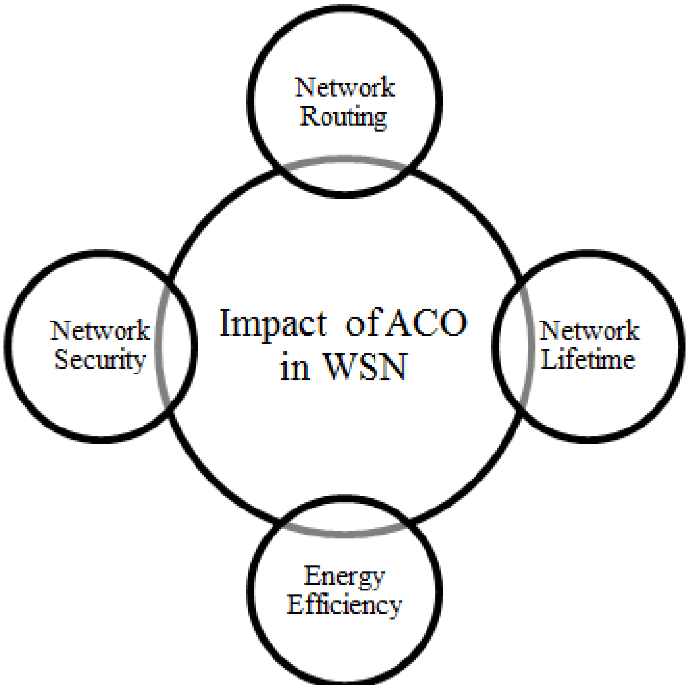

Figure. 1 ACO and WSN

a. ACO and Network Routing

WSNs are extremely versatile and can be deployed in varying density for different applications. Irrespective of the varied objectives of sensor applications, it is necessary that the basic task of sensing, collecting, processing and transmitting of data is done efficiently. This requires the development of energy-efficient routing protocols to set up paths between the sensor nodes and the data sink [1].

Liao et al. proposed an ant colony based algorithm for data aggregation in WSN [8]. All possible paths from the source node to the sink node are explored by every ant. The data aggregation tree is constructed by the accumulation of pheromone. Cobo et al. proposed AntSensNet, an ant-based multi-QoS routing metric for Wireless Multimedia Sensor Networks (WMSN) [9]. The AntSensNet protocol built a hierarchical structure on the network, maximized network utilization and improved the network performance. It had better convergence and provided significantly better QoS for multiple types of services in WMSNs. A detailed survey of swarm intelligence based routing protocol for wireless sensor networks was presented by Saleem et al. in [10]. Critical analysis of the existing protocols and future research directions has also been presented.

Zungeru et al have presented a comprehensive survey and comparison of classical and swarm intelligence based routing protocols in WSNs [11]. The routing protocols were classified based on their computational complexity, network structure, energy efficiency and path establishment. An ACO based ladder diffusion algorithm was proposed by Ho et al. to reduce the power consumption and overcome the transmission routing problems in WSNs [12]. The algorithm also ensured safety and reliability of transmitted data and also provided backup routes. It reduced power consumption by 52.36% and increased the data forwarding efficiency by 61.11% as compared to directed diffusion algorithm.

Ye and Mohamadian proposed adaptive clustering based dynamic routing of WSNs using ACO. This adaptive routing protocol performed well in alleviating network congestion and eliminating data redundancy thus improving energy efficiency [13]. Guo and Zhang presented a survey of all intelligent routing protocols in WSNs which contributed to the optimization of network lifetime. Routing protocols based on Reinforcement Learning (RL), ACO, Fuzzy Logic (FL), Genetic Algorithm (GA) and Neural Networks (NN) have been discussed [14].

A new hybrid ABCACO (Artificial Bee Colony Ant Colony Optimization) algorithm for energy efficient routing in clustered WSNs has been proposed by Kumar et al. in [15]. The proposed technique has been reported to be of use in forest fire detection and monitoring. Zahedi et al. have proposed swarm intelligence based fuzzy routing protocol for clustered wireless sensor networks [16]. The proposed algorithm outperformed the existing clustering-based protocols in generation of balanced clusters and enhancement of network lifetime.

b. ACO and Network Lifetime

The lifetime of WSN depends on the density and rate of communications of sensors. ACO has been used for maximizing the network lifetime in WSN. The autonomy and dynamic deployment of mobile sensor networks was effectively solved using a blackboard mechanism based ant colony theory by Qi and Li in [17]. The algorithm reduced the power consumption by 13%, enhanced the efficiency of path planning and deployment of WSN by 15%. The sensor deployment problem was modeled as multiple knapsack problem by Liao et al. in [18]. The ACO based algorithm, prolonged the network lifetime and ensured full coverage. Five different scenarios were considered for performance evaluation and the simulation results proved that this ACO based algorithm, increased the network lifetime by increasing the energy and density of the sensors closer to the sink.

A novel ACO based routing approach maximizing the lifetime of WSNs have been proposed by Ahmed et al. in [19]. The network parameters for WSN routing have been optimized to provide maximum service life of the network. The proposed approach outperformed the LEACH and AODV protocols.

Castro et al. developed a Bio-Inspired Optimization for Sensor Network Lifetime (BiO4SeL) to perform self-organization and optimization of lifetime by means of routing into a WSN [20]. Bio4SeL increased the sensor lifetime and maintained the best amount of packet delivery, network connectivity and energy saving. An ACO-based approach that maximizes the lifetime of heterogenous WSNs was proposed by Lin et al in [21]. It was based on finding the maximum number of disjoint connected covers that satisfy both sensing coverage and network connectivity.

Sensor deployment of WSN based on ACO with Three Classes of Ant Transitions (ACO-TCAT) was proposed by Liu in [22]. This novel algorithm effectively addressed the problem of minimizing cost and connectivity guaranteed grid coverage. Liu also proposed a novel transmission scheme for WSNs using ACO with unconventional characteristics for maximizing network lifetime [23]. The proposed transmission strategy aimed to maximize energy efficiency and energy balancing.

A novel node deployment approach based on ACO and greedy migration mechanism was proposed by Liu and He in [24]. The problem of Grid-based Coverage with Low cost and Connectivity-guarantee (GCLC) was considered and the proposed approach could complete the full coverage quickly and decrease the deployment cost significantly. It could also balance power consumption among sensor nodes effectively and prolong the network lifetime in grid-based WSNs.

c. ACO and Energy Efficiency

Energy efficiency is a very critical factor in WSN for prolonging network lifetime, improving data aggregation and effective broadcasting. ACO based algorithms for energy efficient WSNs have been presented here.

Woungang et al. presented the design of energy-efficient protocols for wireless ad hoc and sensor networks using ant colony agents [25]. Misra et al. designed an energy-aware routing protocol, incorporating the effect of power consumption in routing a packet and exploiting the multi-path transmission properties of ant swarms, thus increasing the battery life of the node [26]. It was observed that, in the ACO based approach energy per packet was significantly decreased compared to other algorithms. Kumar and Thomas proposed a data collection scheme, Maximum Amount Shortest Path (MASP) as a linear integer programming problem and solved it using improved ant colony optimization [27]. This technique increased the network lifetime and energy efficiency significantly by optimizing the assignment of sensor nodes.

C. Lin et al. proposed a family of energy-efficient Data Aggregation Ant Colony Algorithms (DAACA) [28]. These algorithms include three phases: initialization, packet transmission and operation on pheromones. They showed higher performance on average degree of nodes, energy efficiency, maximization of network lifetime, computation complexity and success ratio of one hop transmission. Hernandez and Blum proposed distributed ant colony optimization for minimum energy broadcasting in sensor networks with realistic antennas [29]. Energy efficiency in the WSN was attained by adjusting the transmission power levels of the sensor nodes' antennas.

Lee et al. proposed energy efficient coverage of WSNs using ACO with three types of pheromones [30]. The proposed Three Pheromones ACO (TPACO) algorithm uses one local pheromone and two global pheromones. The problem of energy efficient coverage of WSN was solved using an Ant-Colony-Based Scheduling Algorithm (ACB-SA) by Lee and Lee [31]. The performance of ACB-SA was improved by applying a new initialization method for the pheromone field and the modified construction graph. Tomar et al. have proposed a fuzzy based ACO approach for WSN with improved energy efficiency, network lifetime and optimal path [32]. Sharma and Grover proposed a modified ant colony optimization (mACO) for energy efficient wireless sensor networks [33]. The proposed strategy finds the optimal energy efficient path for choosing nodes for signal transmission in order to maximize network lifetime.

d. ACO and Network Security

Implementation of security in WSN is a highly challenging task. ACO has been successfully used in network security too. Dhurandher et al. proposed a quality-based distance vector routing (QDV), based on ACO for securing the WSN [34]. Quality-of-Service (QoS) and reputation are the two fundamental parameters used. An improved ACO-based security routing protocol for WSN was proposed by Luo et al. in [35]. The node trust value was effectively evaluated using fuzzy logic. Trust value and residual energy of nodes were used to increment the pheromone in the ant colony algorithm.

Sreelaja and Vijayalakshmi presented swarm intelligence based approach for sinkhole attack detection in wireless sensor networks [36]. They proposed an Ant Colony Optimization Attack Detection (ACO-AD) algorithm to identify the sinkhole attacks based on nodeids defined in the ruleset.

IV. TRUST MANAGEMENT IN WSN

The necessity of trust in a WSN is basically applicable for sensing, data disclosure decisions and key exchange [37]. Trust established between two nodes augurs well for collaboration between them, reduction of uncertainty, assist in key management activities and other security mechanisms. Hence, it is imperative that that trust of a node is modeled properly.

A brief survey of the research works done in modeling of trust in a WSN is presented here. Marmol and Perez presented a pre-standardization of trust and reputation models for distributed and heterogenous systems [38]. An interface proposal for trust and/or reputation models has been proposed after making a global comparison of relevant models. Boukerch et. al. developed a novel Agent-based Trust and Reputation Management (ATRM) scheme to WSN [39]. They proved that trust and reputation can be calculated in a WSN with minimum overhead. Modeling and evaluation of trust in WSN based on entropy has been proposed by Hongjun et al [40]. An entropy based trust management scheme for the purpose of data collection in WSNs has been proposed by Luo et al in [41]. A Group-based Trust Management Scheme (GTMS) for WSNs has been developed by Shaikh et al in [42]. This new approach reduced the trust evaluation costs, demanded less memory, energy and communication overhead. Momani et. al. proposed a new Bayesian fusion algorithm to infer the overall trust between the nodes in a WSN in [43]. They calculated the trust value using two trust components namely data trust and communication trust.

A Bio-inspired Trust and Reputation Model called BTRM-WSN, based on ant colony systems have been proposed by Marmol and Perez, in order to provide trust and reputation in WSN [6]. A resilient trust model for hierarchical WSN, with importance on data integrity and known as SensorTrust has been developed by Zhan et al in [44]. This model uses a Gaussian model to rate the data integrity and calculates the current trust level by integrating the past history and recent risks. A trust model based on fuzzy logic has been proposed for WSN by Kim and Seo in [45]. The fuzzy model has been applied to show how the mechanism of trust helps in choosing the right path from source to destination. The overall trust of a sensor node is evaluated using the trust attributes from the communication and social networks and a cluster-based hierarchical trust management protocol for WSNs has been proposed by Bao et al in [46]. The developed protocol has been successfully applied for trust-based routing and intrusion detection. A detailed survey on the applications of various trust and reputation based models for security has been presented by Kumar et al in [47].

Li et al. proposed a Lightweight and Dependable Trust System (LDTS) for clustered WSN. This approach outperformed the drawbacks of conventional weighting methods for trust factors [48]. The power consumption and resource utilization of a trust and reputation model deployed in a WSN has been investigated and reported by Singh et al. in [49]. A robust trust establishment scheme for WSNs was proposed by Ishmanov et al. in [50]. A simple trust estimation method has been employed considering the vulnerability of trust establishment. Jiang et al. proposed an Efficient Distributed Trust Model (EDTM) for WSNs for accurate evaluation of the trustworthiness of the nodes and for more effective prevention of node compromise [51]. In this paper, three different trust models have been used to initialize the trust value of the network.

a. Trust Model based on four components

In Bao et al., the overall trust of a sensor node is calculated using multidimensional attributes of trust obtained from social and communication networks [46]. The trust value that node *i* evaluates towards node *j* at time *t*, $T_{ij}(t)$ as calculated in (5) is represented as a real number in the range [0,1], where 1 indicates complete trust, 0.5 ignorance and 0 distrust.

$$\begin{aligned} T_{ij}(t) = 0.5 w_{social}\left[T_{ij}^{\text{int}imacy}(t) + T_{ij}^{honesty}(t)\right] + \\ 0.5 w_{QoS}\left[T_{ij}^{energy}(t) + T_{ij}^{unselfishness}(t)\right] \end{aligned} \qquad (5)$$

with $w_{social}+w_{QoS} = 1$.

b. Entropy Trust Model

In Hongjun et al., entropy which is basically a concept in thermodynamics and statistical mechanics has been used to build a trust model for WSN [40]. The measure of trustworthiness of is defined by (6).

$$T(H(p)) = \begin{cases} \dfrac{H(p)}{2} & 0 \le H(p) < 0.5 \\ 1 - \dfrac{H(p)}{2} & 0.5 \le H(p) \le 1 \end{cases} \qquad (6)$$

where $H(p) = -p\log_2 p-(1-p)\log_2(1-p)$ and p is the probability for the action to be performed.

c. Fuzzy Trust Model

A trust model based on fuzzy logic is built by Kim and Seo [45]. To calculate the value of trust of a sensor node, T is defined as trustworthiness and U is defined as untrustworthiness whose ranges are given by $0 \le T \le 1$ and $0 \le U \le 1$. The trust and untrust values are calculated as in (7).

$$\begin{aligned} T &= \frac{avg(T_i, T_j)}{1-(avg(T_i, U_j) + avg(T_j, U_i))} \\ U &= \frac{avg(U_i, U_j)}{1-(avg(T_i, U_j) + avg(T_j, U_i))} \end{aligned} \qquad (7)$$

and the final value of trust of the sensor network is evaluated as given in (8).

$$Evaluation\_value = \frac{T}{T+U} \tag{8}$$

V. ACO BASED EVALUATION OF TRUST MODELS FOR WSNs

In this paper, three different hybrid trust models for WSNs have been built based on equations (5), (6), (7) and (8). These models are used for initialization of the trust values of a network. The updation of the trust values and the discovery of the shortest path for packet delivery within the network is performed by the Ant Colony Optimization algorithm. The performance of these hybrid models are measured using path length, trust calculation and energy consumption. The response of these models to bad mouthing attack and Sybil attack has also been analyzed.

a. Security Threats

The important purpose of securing a network is to protect it from various internal and external attacks. According to Yu et al., in external attacks, the enemy either tries to eavesdrop information or injects unwanted data into the network or creates non-existent records to disturb the normal functioning of the network [52]. The sniffing attack and hello flood attack are examples of external attacks. In internal attacks, the enemy breaks open the traditional cryptographic security and authentication mechanisms, capture the sensor nodes and disrupt the working of the network. Sinkhole attack, stealthy attack and bad mouthing attack are examples of internal attacks [52]. They are few attacks like the blackhole attack, energy drain attack and the sybil attack that can be classified under both internal and external attacks. Marmol and Perez [53] have presented various security threats scenarios in trust and reputation models for distributed systems.

The behavior of the hybrid trust models developed for routing of data packets, have been tested using two different attacks namely the bad mouthing attack and the sybil attack.

Bad mouthing attack: The bad mouthing attack implies the propagation of negative information about good nodes [52]. The consequence of this attack is that valid and highly trusted paths may not be traversed because of the wrong information propagated. This is an internal attack and will definitely increase the energy consumption of the network.

Sybil attack: Sybil attack is also known as node replication attack. It clones several nodes and returns replicas by capturing at least one node [52]. The important consequences of this attack are that the links between valid nodes are overheard and power energy of nodes is exhausted.

VI. RESULTS AND DISCUSSIONS

The proposed hybrid trust models are tested for routing application. The WSN under study includes 100 nodes distributed across an area of 100x100. The range of each node is 20m. The trust values of the sensor nodes are initialized using three different models. The updation of trust values and determination of the shortest path for packet delivery is undertaken by the ACO algorithm. The validity of the path taken is calculated by evaluating the total trust of the path taken and the energy consumed in the process.

a. Energy Consumption

Energy consumption is a very important issue pertaining to WSNs. As the sensors in the WSNs are involved in sensing, processing and communicating, they are highly resource-constrained. Generally, the power required by a sensor in a WSN can be seen as function of the distance [6]. The energy required by a sensor r to deliver a packet to a sensor s at a distance d is:

$$E(d) = d^{\alpha} + C \qquad (9)$$

where $\alpha \in [2,6]$ denotes the media attenuation factor and C is a constant representing the power used to process the radio signal. C has been taken as being equal to 10^8.

b. Analysis of Results

Table 1 shows the results of the tests performed. The parameters used for the ACO algorithm are $\alpha=0.1$, $\beta=2$, $\rho=0.1$ and $Q=1$. The value of τ is initialized as the trust values from the three different trust models.

Table 1: Performance of Trust Models

Trust Model		Path Length (m)	Trust Value	Energy consumed (J)
Trust components +ACO	Normal	1563.3	0.4962	1.0535×10^{7}
	Bad Mouthing	1591.6	0.4691	1.3016×10^{8}
	Sybil	1619.4	0.2970	1.08×10^{8}
Entropy model + ACO	Normal	1104.7	0.4950	1.4916×10^{12}
	Bad Mouthing	1116.2	0.4518	3.9518×10^{9}
	Sybil	1132.8	0.2970	1.0142×10^{9}
Fuzzy trust model + ACO	Normal	1540.6	0.4950	4.6203×10^{9}
	Bad Mouthing	1565.6	0.4724	3.326×10^{11}
	Sybil	1551.6	0.2973	7.056×10^{11}

The algorithm was run for 200 iterations. It was observed that for all the three models the path length covered during normal conditions is the shortest. The path length taken for data delivery during bad mouthing attack and Sybil attack is more for all the models. Among the three models, the model based on entropy and ACO gives the shortest path length for all the conditions. The trust value of the path taken symbolizes that the quality of the path travelled is least during Sybil attack for all the three models. The hybrid model based on trust components and ACO shows least energy consumption under all conditions.

The developed hybrid models have withstood the impacts of the two attacks under study and have performed considerably well.

VII. CONCLUSION

A brief survey of the application of ACO in network routing, network lifetime, energy efficiency and network security has been presented. The necessity of various trust models for security in WSNs has also been discussed. Hybrid trust models based on ACO algorithm have been proposed and their performance was tested for routing application, when a packet has to be delivered from one node to the other in a WSN. The hybrid model based on entropy and ACO registers the shortest path. The quality of the path taken was evaluated by calculating the overall trust value of the path. The energy consumption which is one of the important constraints of a WSN has also been calculated. Hybrid model based on various trust components and ACO registers the highest trust value and least energy consumed. Better models can be built with suitable changes for different trust-based applications.

REFERENCES

[1] K. Sohraby, D. Minoli, T. Znati, "Wireless sensor networks: Technology, Protocols and Applications", John Wiley and Sons: New Jersey, 2007

[2] G. Edwin Prem Kumar, K. Baskaran, R. Elijah Blessing Rajsingh, "Research issues in wireless sensor network applications: A survey", International Journal of Information and Electronics Engineering, Vol. 2, No. 5, pp. 702-706, 2012.

[3] S. Jabbar, R. Iram, A. A. Minhas, I. Shafi, S. Khalid, M. Ahmad, "Intelligent optimization of wireless sensor networks through bio-inspired computing: survey and future directions", Intl. J. of Distributed Sensor Networks, pp. 1 – 13, 2013.

[4] M. A. Adnan, M. A. Razzaque, I. Ahmed, I. F. Isnin, "Bio-mimic optimization strategies in wireless sensor networks: A survey", J. of Sensors, Vol. 14, pp. 299-345, 2014.

[5] M. Dorigo, L. M. Gambardella, "Ant Colony System: A cooperative learning approach to the traveling salesman problem", IEEE Transactions on Evolutionary Computation, Vol. 1, No.1, pp. 53-66, 1997.

[6] F. G. Marmol, G. M. Perez, "Providing trust in wireless sensor networks using a bio-inspired technique", Telecommunication Systems, Vol. 46, pp. 163 – 180, 2011.

[7] M. Dorigo, M. Birattari, T. Stutzle, "Ant colony optimization: Artificial ants as a computational intelligence technique", IEEE Computational Intelligence Magazine, pp. 28-39, 2006.

[8] W. Liao, Y. Kao, C. Fan, "Data aggregation in wireless sensor networks using ant colony algorithm", J. Network and Computer Applications, Vol. 31, pp. 387-401, 2008.

[9] L. Cobo, A. Quintero, S. Pierre, "Ant-based routing for wireless multimedia sensor networks using multiple QoS metrics", Computer Networks, Vol. 54, pp. 2991-3010, 2010.

[10] M. Saleem, G. A. Di Caro, M. Farooq, "Swarm Intelligence based routing protocol for wireless sensor networks: Survey and future directions", J. Information Sciences, Vol. 181, pp. 4597-4624, 2011.

[11] A. M. Zungeru, L. Ang, K. P. Seng, "Classical and swarm intelligence based routing protocols for wireless sensor networks: A survey and comparison", J. Network and Computer Applications, Vol. 35, pp. 1508 – 1536, 2012.

[12] J. Ho, H. Shih, B. Liao, S. Chu, "A ladder diffusion algorithm using ant colony optimization for wireless sensor networks", J. Information Sciences, Vol. 192, pp. 204-212, 2012.

[13] Z. Ye, H. Mohamadian, "Adaptive clustering based dynamic routing of wireless sensor networks via generalized Ant Colony Optimization", Intl. Conf. on Future Information Engineering, IERI Procedia, Vol. 10, pp. 2-10, 2014.

[14] W. Guo, W. Zhang, "A survey on intelligent routing protocols in wireless sensor networks", J. Network and Computer Applications, Vol. 38, pp. 185-201, 2014.

[15] R. Kumar, D. Kumar, "Hybrid swarm intelligence energy efficient clustered routing algorithm for wireless sensor networks", Journal of sensors, pp. 1-19, 2016.

[16] Z. M. Zahedi, R. Akbari, M. Shokouhifar, F. Safaei, A. Jalali, "Swarm intelligence based fuzzy routing protocol for clustered wireless sensor networks", Expert Systems with Applications, Vol. 55, pp. 313-328, 2016.

[17] G. Qi, P. Song, K. Li, "Blackboard mechanism based ant colony theory for dynamic deployment of mobile sensor networks", J. Bionic Engineering, Vol. 5, pp. 197-203, 2008.

[18] W. Liao, Y. Kao, R. Wu, "Ant colony optimization based sensor deployment protocol for wireless sensor networks", Expert Systems with Applications, Vol. 38, pp. 6599-6605, 2011

[19] B. M. Ahmed, A. A. Boudhir, M. BouHorma, "New routing algorithm based on ACO approach for lifetime optimization in wireless sensor networks", Intl. J. of Networks and Systems. Vol. 1, No. 2, pp. 64-67, 2012.

[20] M. Castro, L. Ribeiro, C. Oliveira, "An autonomic bio-inspired algorithm for wireless sensor network self-organization and efficient routing", J. Network and Computer Applications, Vol. 35, pp. 2003-2015, 2012.

[21] Y. Lin, J. Zhang, H. S. Chung, W. H. Ip, Y. Li, Y. Shi, "An ant colony optimization approach for maximizing the lifetime of heterogenous wireless sensor networks", IEEE Trans. on Systems, Man and Cybernetics – Part C: Applications and Reviews, Vol. 42, No. 3, pp. 408-420, 2012.

[22] X. Liu, "Sensor deployment of wireless sensor networks based on ant colony optimization with three classes of ant transitions", IEEE Communications Letters, Vol. 16, No. 10, pp. 1604-1607, 2012.

[23] X. Liu, “A transmission scheme for wireless sensor networks using ant colony optimization with unconventional characteristics”, IEEE Communication Letters, Vol. 18, No. 7, pp. 1214-1217, 2014.

[24] X. Liu, D. He, “Ant colony optimization with greedy migration mechanism for node deployment in wireless sensor networks”, J. Network and Computer Applications, Vol. 39, pp. 310-318, 2014.

[25] I. Woungang, S. K. Dhurandher, M.S. Obaidat, “Using Ant Colony Agents for Designing Energy-Efficient Protocols for Wireless Adhoc and Sensor Networks”, Handbook of Green Information and Communication Systems, Academic Press, 2012.

[26] S. Misra, S. K. Dhurandher, M. S. Obaidat, P. Gupta, K. Verma, P. Narula, “An ant swarm-inspired energy-aware routing protocol for wireless ad-hoc networks”, J. Systems and Software, Vol. 83, No. 11, pp. 2188-2199, 2010.

[27] A. Kumar, A. Thomas, “Energy efficiency and network lifetime maximization in wireless sensor networks using improved ant colony optimization”, Procedia Engineering, Vol. 38, pp. 3797-3805, 2012.

[28] C. Lin, G. Wu, F. Xia, M. Li, L. Yao, Z. Pei, “Energy efficient ant colony algorithms for data aggregation in wireless sensor networks”, J. Computer and System Sciences, Vol. 78, pp. 1686-1702, 2012.

[29] H. Hernandez, C. Blum, “Distributed Ant Colony Optimization for Minimum Energy Broadcasting in Sensor Networks with Realistic Antennas”, J. Computers and Mathematics with Applications, Vol. 64, pp. 3683-3700, 2012.

[30] J. W. Lee, B. S. Choi, J. J. Lee, “Energy-efficient coverage of wireless sensor networks using ant colony optimization with three types of pheromones”, IEEE Trans. on Industrial Informatics, Vol. 7, No. 3, pp. 419 -427, 2011.

[31] J. W. Lee, J. J. Lee, “Ant-colony-based scheduling algorithm for energy-efficient coverage of WSN”, IEEE Sensors Journal, Vol. 12, No. 10, pp. 3036 – 3046, 2012.

[32] G. S. Tomar, T. Sharma, B. Kumar, “Fuzzy based ant colony optimization approach for wireless sensor network”, Wireless Personal Communications, Vol. 84, pp. 361-375, 2015.

[33] V. Sharma, A. Grover, “A modified ant colony optimization algorithm (mACO) for energy efficient wireless sensor networks”, Optik, Vol. 127, pp. 2169-2172, 2016.

[34] S. K. Dhurandher, S. Misra, M. S. Obaidat, N. Gupta, "An ant colony optimization approach for reputation and quality-of-service-based security in wireless sensor networks", J. Security and Communication Networks, Vol. 2, No. 2, pp. 215-224, 2009.

[35] Z. Luo, R. Wan, X. Si, "An improved ACO-based security routing protocol for wireless sensor networks", Intl. Conf. Computer Sciences and Applications, pp. 90-93, 2013.

[36] N. K. Sreelaja, G. A. Vijayalakshmi Pai, "Swarm Intelligence based approach for sinkhole attack detection in wireless sensor networks", J. Applied Soft Computing, Vol. 19, pp. 68-79, 2014.

[37] J. Lopez, R. Roman, I. Agudo, C. F. Gago, "Trust management systems for wireless sensor networks: Best practices", Computer Communications, Vol. 33, pp. 1086-1093, 2010.

[38] F. G. Marmol, G. M. Perez, "Towards pre-standardization of trust and reputation models for distributed and heterogenous systems", J. Computer Standards and Interfaces, Vol. 32, pp. 185-196, 2010.

[39] A. Boukerch, L. Xu, K. El-Khatib, "Trust-based security for wireless adhoc and sensor networks", Computer Communications, Vol. 30, pp. 2413-2427, 2007.

[40] D. Hongjun, J. Zhiping, D. Xiaona, "An entropy-based trust modeling and evaluation for wireless sensor networks", Intl. Conf. on Embedded and Software and Systems, pp. 27-34, 2008.

[41] H. Luo, J. Tao, Y. Sun, "Entropy-based trust management for data collection in wireless sensor networks", 5th Intl. Conf. on wireless communications, networking and mobile computing, pp. 1-4, 2009.

[42] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, Y. J. Song, "Group-based trust management scheme for clustered wireless sensor networks", IEEE Trans. on Parallel and Distributed Systems, Vol. 20, No. 11, pp. 1698 -1712, 2009.

[43] M. Momani, S. Challa, R. Alhmouz, "Bayesian fusion algorithm for inferring trust in wireless sensor networks", Journal of Networks, Vol. 5, No. 7, pp. 815 – 822, 2010.

[44] G. Zhan, W. Shi, J. Deng, "SensorTrust: A resilient trust model for wireless sensing systems", Pervasive and Mobile Computing, Vol. 7, pp. 509-522, 2011.

[45] T. K. Kim, H. S. Seo, "A trust model using fuzzy logic in wireless sensor network", World Academy of Science, Engineering and Technology, Vol. 18, pp. 63-66, 2008.

[46] F. Bao, I. R. Chen, M. Chang, J. H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection”, IEEE Transactions on Network and Service Management, Vol. 9, No. 2, pp. 169-183, 2012.

[47] G. Edwin Prem Kumar, I. Titus, I. T. Sony, “A comprehensive overview on application of trust and reputation in wireless sensor network”, Procedia Engineering, Vol. 38, pp. 2903-2912, 2012.

[48] X. Li, F. Zhou, J. Du, “LDTS: A Lightweight and Dependable Trust System for clustered wireless sensor networks”, IEEE Trans. on Information Forensics and Security, Vol. 8, No. 6, pp. 924-935, 2013.

[49] S. Singh, V. K. Verma, N. P. Pathak, “Sensors augmentation influence over trust and reputation models realization for dense wireless sensor networks”, IEEE Sensors Journal, Vol. 15, No. 11, pp. 6248-6254, 2015.

[50] F. Ishmanov, S. W. Kim, S. Y. Nam, “A robust trust establishment scheme for wireless sensor networks”, Journal of Sensors, Vol. 15, pp. 7040-7061, 2015.

[51] J. Jiang, G. Han, F. Wang, L. Shu, M. Guizani, “An efficient distributed trust model for wireless sensor networks”, IEEE Trans. on Parallel and Distributed Systems, Vol. 26, No. 5, pp. 1228-1237, 2015.

[52] Y. Yu, K. Li, W. Zhou, P. Li, “Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures”, J. Network and Computer Applications. Vol. 35, pp. 867-880, 2012.

[53] F. G. Marmol, G. M. Perez, “Security threats scenarios in trust and reputation models for distributed systems”, J. Computers and Security, Vol. 28, pp. 545-556, 2009.