GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ANT COLONY OPTIMIZATION (ACO) MECHANISM FOR TRUST AND REPUTATION MANAGEMENT IN WIRELESS SENSOR NETWORKS

R.SHARMILA
Department of computer science and Engineering, Bharathidasan University

ABSTRACT

Wireless Sensor Network (WSN) is an emerging technology and explored field of researchers worldwide in the past few years, so does the need for effective security mechanisms. The major challenge faced by wireless sensor networks is security. Because of dynamic and collaborative nature of sensor networks the connected sensor devices makes the network unusable.. However, the wireless sensor networks themselves are prone to security attacks. The list of security attacks, although already very long, continues to augment impeding the expansion of these networks. The trust management schemes consist of a powerful tool for the detection of unexpected node behaviors (either faulty or malicious). Once misbehaving nodes are detected, their neighbors can use this information to avoid cooperating with them, either for data forwarding, data aggregation or any other cooperative function. This study focuses on trust and reputation management by Ant Colony Optimization (ACO) algorithm based on biological inspired technique. The objective of the current proposed system is to provide an efficient reputation and trust solution to WSN which can provide a high level of security. This paper will also cover an overview of WSNs architecture, challenges in WSN, existing trust models and their security issues.

Keywords— Wireless Sensor Networks, Trust And Reputation, BTRM-WSN, Ant colony Optimization(ACO).

I. INRODUCTION

Wireless sensor networks are network of thousand of sensor nodes. Sensor nodes are small in size,less memory space, cheaper in price with restricted energy source and limited processing capability.

Wireless sensor networks today offer the processing capabilities of computers of a few decades ago and the industry's trend is to reduce the cost of wireless sensing nodes while maintaining the same processing power. Our proposed model is based on a bio-animated algorithm called ant colony optimization (ACO) where ants build paths fulfilling certain conditions in a graph (equally, in a network). These ants leave some pheromone traces that help next ants to node and follow those routes. This section B will cover an overview of WSNs architecture, Section B will cover existing trust models and their security issues.

Exploring the symbiotic nature of biological systems can result in valuable knowledge for computer networks. Biologically animated techniques seem promising because of their intrinsic appealing characteristics as self-healing, self-adapting, and self-evolving. They are better because the techniques are more robust at the time of communication errors when optimized systems fail to deliver optimum performance. While closely looking at nature, we can derive inspiration from everything we see [4]. May it be from animals, birds, waterfall, etc. Birds' flock together synchronizing their pattern, bees perform nectar search with a well-defined procedure, and ants find their food source with the stigmergy. All these social insects along with numerous examples have been studied thoroughly and are used in deriving inspiration in various fields. Effective management of constrained resources with a globally amplified intelligence.

Characteristics of biological system:

- Task allocation process in insect colonies
- Able to self-organize in a fully distributed fashion Activator-inhibitor systems
- Collaboratively achieving efficient equilibrium
- Homeostatic system
- Survivable to harsh conditions with inherent and sufficient redundancy
- Epidemic spreading

In this paper organized as follows. Section A describes overview of WSNs architecture. Section B presented some Challenges in WSN. Section C deals with trust and reputation and how it monitored. Section D reviews various existing trust and reputation models. Section E elaborates the ant colony optimization .section F describes BTRM-WSN trust and reputation based on ACO and then finally conclusion of this paper.

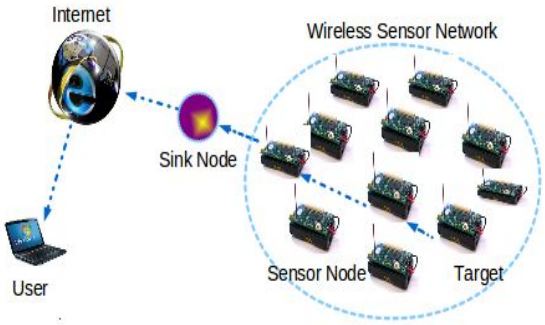


Figure 1: Wireless sensor network

II. WIRELESS SENSOR NETWORK ARCHITECTURE

Sensor motes (Field devices):

Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.

Gateway or Access points:

Gateway enables communication between Host application and field devices.

Network manager:

A Network Manager is responsible for configuration of the network, scheduling communication between devices management of the routing tables and monitoring and reporting the health of the network.

Security manager:

The Security Manager is responsible for the generation, storage, and Management of keys.

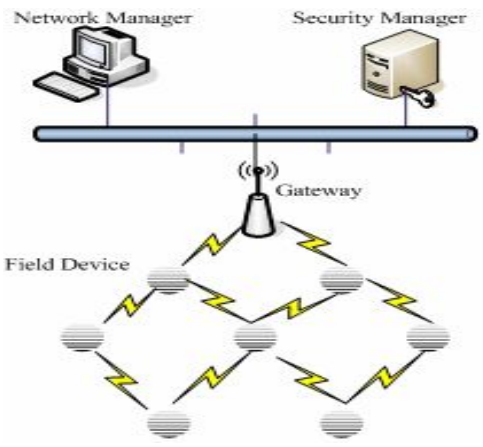


Figure 2: Architecture of WSN

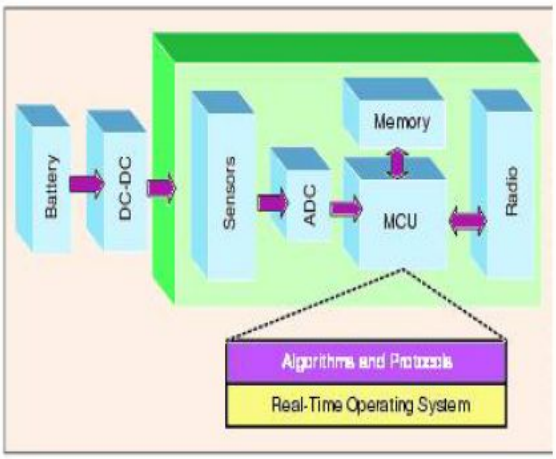


Figure 3:System architecture of a typical wireless sensor node

III. CHALLENGES IN WSN

Energy Support

Most important restraint in a WSN is limited energy support of sensor nodes. Since sensor nodes are deployed in adhoc manner and after deployment they left unattended. So initial battery power is the main source of their lifetime survival. Once sensor nodes are deployed they could not be recharged. So today to establish an energy efficient wireless sensor network is a great issue and a challenge.

In Real Time Environment

WSN deal with real world environments. In many cases, sensor data must be delivered within time constraints so that appropriate observations can be made or actions taken. Very few results exist to date regarding meeting real-time requirements in WSN.

Ad-Hoc Deployment

Sensor nodes are distributed randomly in required monitoring field. For example –for monitoring forest activities sensor nodes are dropped from the plane. Then sensor nodes itself create connections with other nodes and form an infrastructure. Hence new standards and protocols should be developed to maintain this type of ad-hoc network.

Wireless Channel

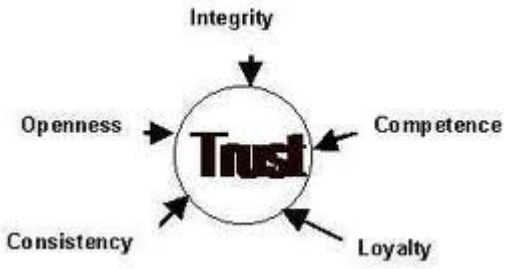
The wireless channel is unreliable in nature, and a number of phenomena can prevent a transmitted packet from reaching a receiver. One such phenomenon is interference. If two independent transmitters transmit on the same channel such that their signals overlap, they may corrupt each other's signal at a receiver's radio. This requires the transmitter to re-transmit, at the cost of additional time and energy. So to maintain efficient wireless channel is a great challenge today.

Fault Tolerance

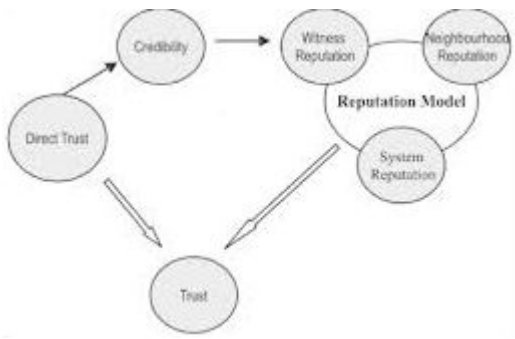
Sensor nodes are prone to failure because of unattended environment. A sensor node may fail due to hardware or software problem or energy exhaustion. If a few of sensor nodes fail, working protocol should handle this type of fault tolerance.

IV. TRUST AND REPUTATION

The use of the words "trust" and "reputation" is commonplace in our daily lives. The repute of a person is established from previously performed actions. If a person is consistently honest, then with time, his or her reputation would be good, and everybody would trust him or her.



In practice, **trust** is defined as how much a node matches the expectations of another node. The concept of trust is especially important in an environment where there is some degree of uncertainty. In WSNs, the nodes are always at risk of being compromised by an adversary. The most common applications of trust in WSNs include, but are not limited to, malicious node identification, secure routing, secure cluster head selection, and secure data collect.



The **reputation** is the collective trust opinion of other nodes about the behavior of a subject node. In other words, reputation may be understood as the trustworthiness of a node.

V. TRUST AND REPUTATION MONITORING SYSTEM

A system that makes the use of trust and reputation information to calculate the trustworthiness of a node is called a TRM.

Bootstrapping:

A TRM may be initialized in three ways by considering thefollowing: (i) each network node as trustworthy, (ii) all nodes as untrustworthy, and (iii) each node having a neutral trust rating.

Observation—firsthand and secondhand information

In a TRM, the nodes may share two types of information, namely, firsthand and secondhand. Firsthand information is the node's personal experience through a direct interaction with the neighboring node. Alternatively, indirect information is provided to the node by other nodes on the basis of their own experiences with the subject node.

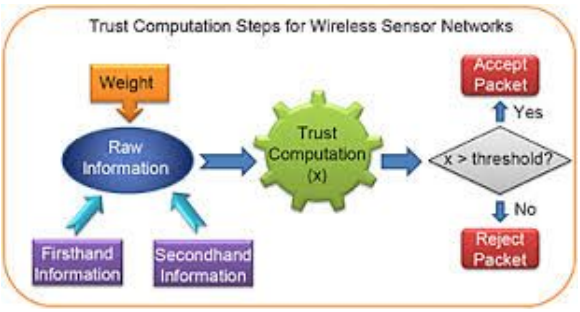
Centralized and distributed trust and reputation monitoring

If trust and reputation are accumulated and stored by as ingle entity in the whole network, then the TRM is called centralized.

Trust computation steps

Typically, a TRM performs the following steps for the computation of trust:

- information collection,
- information dissemination,
- information mapping to trust model, and
- decision making



VI. EXISTING TRUST REPUTATION MANAGEMENT

Collaborative reputation mechanism

Collaborative reputation mechanism (CORE) is a distributed trust model, in which reputation is calculated from the firsthand and secondhand information. Each node within the system maintains a trust table that holds the positive or negative repute for other nodes.

Task-based trust for sensor networks

Boukerche and Li suggested that when an intruder node is detected, then the intruder is blocked by all of the neighbors, regardless of the specific task in which the intruder node was misbehaving. In task-based trust for sensor networks, a node maintains the task-based trust value of the neighboring nodes.

Distributed event-triggered trust Management

a model in which each network node has a set of modules to parse and store trust-related information for the neighboring nodes. A network node maintains a set of information parameters that consists of (i) a public key (shared among neighbors), (ii) reputation, (iii) remaining energy, and (iv) network paths

CONFIDANT framework

The distributed trust nature of "Cooperation of Nodes—Fairness in Dynamic Ad hoc NeTworks" (CONFIDANT) allows each node in the network to maintain both firsthand and secondhand trust information about the neighboring nodes. Each node in CONFIDANT scheme consists of four major components, namely, (i) Monitor, (ii) Trust Manager, (iii) Reputation System, and (iv) Path Manager.

Robust reputation system

Robust reputation system is an improved version of CONFIDANT, presented by the same authors. In the proposed scheme, the authors have included both positive and negative reputation values to avoid false
praise and bad-mouth attacks. For the computation of
repute, Bayesian framework is used along with the Beta distribution. Whenever a node receives secondhand information, the latter is subjected to a deviation test, the success of which indicates authenticity of the information.

Distributed reputation-based beacon trust system trust framework

In a WSN, it is important for the nodes to transmit accurate location information. The model consists of two major components, namely,(i) the beacon nodes and (ii) the sensor nodes. Beacon nodeshave pre-identified locations, whereas the location of a sensor node is computed using a mathematical triangulation method. In triangulation, a sensor node broadcasts the location request and enters into a promiscuous mode.

Agent-based trust and reputation monitoring scheme

In the agent-based trust and reputation monitoring framework, applied trust and reputation to a clustered WSN. In the system, each node is installed with a software component, known as mobile agent, that is responsible for the computation of trust. Whenever two nodes need to interact, the mobile agents on the respective nodes perform a one-to-one communication to exchange reputation information.

VII. ANT COLONY OPTIMIZATION

In analogy with biological system, the individual alone is of less interest compared to the collective behavior of the system of a great number of alike individuals. This line of thinking has led to the foundation of the science and engineering discipline: swarm intelligence to describe the self-organizing properties of such system. At the same time, communication networks are subject to failure either by device and link malfunction or misuse of their capacity.

Swarms

- Swarm of bees
- Ant colony as swarm of ants
- Flock of birds as swarm of birds
- Traffic as swarm of cars
- Immune system as swarm of cells
- and molecules

Swarm Intelligence/Agent Based Modeling

- Model complex behavior using simple agents
- Technique for solving problems which can be expressed as finding good paths through graphs
- Each ant tries to find a route between its nest and a food source

The behavior of each ant in nature

- Wander randomly at first, laying down a pheromone trail
- If food is found, return to the nest laying down a pheromone trail
- If pheromone is found, with some increased probability follow the pheromone trail
- Once back at the nest, go out again in search of food

However, pheromones evaporate over time, such that unless they are reinforced by more ants, the pheromones will disappear.

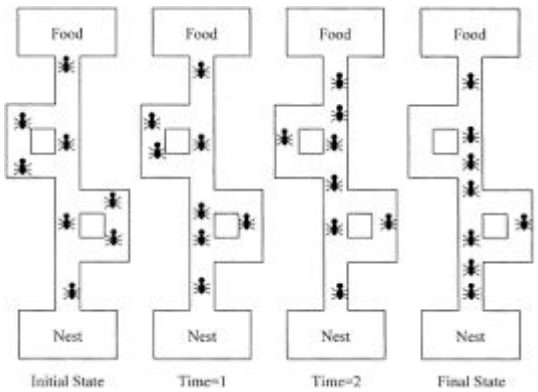


Figure 4-Ant colony optimization

Time1- The first ant wanders randomly until it finds the food source , then it returns to the nest , laying a pheromone trail
Time 2- Other ants follow one of the paths at random, also laying pheromone trails. Since the ants on the shortest path lay pheromone trails faster, this path gets reinforced with more pheromone, making it more appealing to future ants.
Final - The ants become increasingly likely to follow the shortest path since it is constantly reinforced with a larger amount of pheromones. The pheromone trails of the longer paths evaporate.

Table 1. Notation of Nature and Computer Science

Nature	Computer Science
Natural habitat	Graph (nodes and edges)
Nest and food	Nodes in the graph: start and destination
Ants	Agents, our artificial ants
Visibility	The reciprocal of distance, η
Pheromones	Artificial pheromones ,τ
Foraging behavior	Random walk through graph (guided by pheromones)

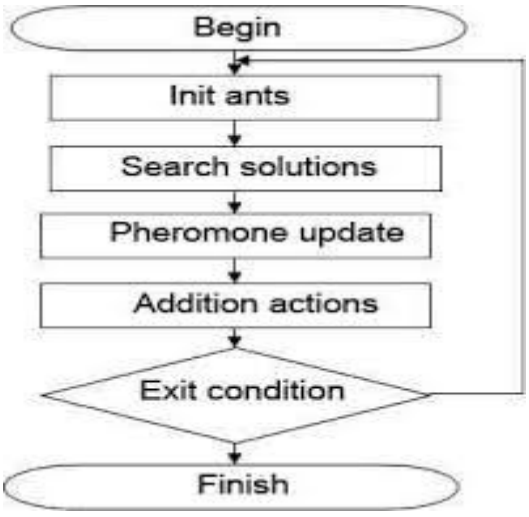


Figure 5:Ant colony system Flow chart

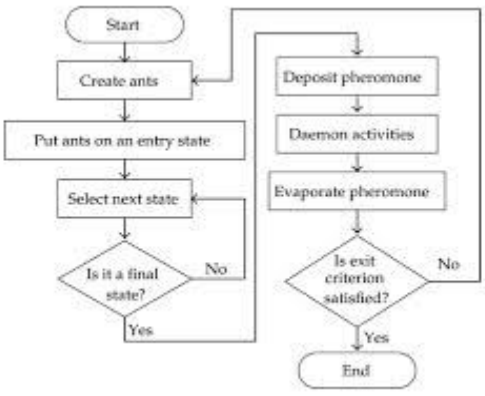


Figure 6:Ant Colony Algorithm Flowchart

Algorithm:

for i = 1 to number of cycles do
for k = 1 to the number of ants do
Ant K solution obtained ← initial node
for i = 2 to the number of nodes do
for k = 1 to the number of ants do
Ant to get the solution K ← (ant K solution obtained) ∪ (next node selection strategy)
Update the local information
for k = 1 to the number of ants do
if (ant K get the quality of path > current best path quality) then
Current best path quality ← Sk
if (current best path quality> global best path quality) then
The global best path quality ← Current best path quality
for i = 1 to number of nodes do
Update the global information
Return the global best path quality.

VIII. BTRM-WSN TRUST AND REPUTATION MODEL BASED ON ANT COLONY OPTIMIZATION

This trust model for wireless sensor networks (WSN) is based on the bio-inspired algorithm of ant colony system In this model, most trustworthy path leads to find the most
reputable service provider in a network. WSN launches a set of artificial agents while searching for a most reputable service provider. In order to carry out a decision about next sensor, probability is given to each arc by the following Eq.(1).

$$pk(r.s) = \begin{cases} \frac{[\tau_{rs}]^{\alpha}[\eta_{rs}]^{\beta}}{\sum[\tau_{ru}]^{\alpha}[\eta_{ru}]^{\beta}} & if\ s \in Jk(r): \\ otherwise & 0 \end{cases} \quad (1)$$

where pheromone value, denotes the heuristic associated with the link joining r and s, $Jk(r)$ represents the set of neighbors of node r not visited yet by ant k, and α , β
parameters balancing the pheromone and the heuristic. The next Eq.(2) represents modification of the ants pheromone trace.

$$\tau_{s1s2} = (1 - \varphi)\tau_{s1s2} + \hat{\varphi}\,\Omega \quad (2)$$

where $\Omega = (1+(1 - \varphi)(1- \tau s1s2\ \eta s1s2))\ \tau s1s2$ denotes the
convergence value of τs1s2 and φ represents a parameter
controlling the amount of pheromone. The best path found by all ants is indicated by Eq.(3).

$$\tau_{rs} = (1-\rho)\tau_{rs} + \rho\left(1 + \tau_{rs}\eta_{rs}Q\left(S_{Global_{Best}}\right)\right)\tau_{rs} \quad (3)$$

where $Q(SGlobal\_Best)$ denotes path quality. The quality of the Sk paths can be measured as the average of all the edges belongs to that path as depicted by Eq.(4).

$$Q(S_k) = \frac{\tau k}{\sqrt{Length(S_k)}}\%A_k \quad (4)$$

where $\%Ak$ denotes the percentage of trustworthy paths. The punishment or rewards of the path leading to the selected peer is given by Eq.(5).

$$\tau_{rs} = (\tau_{rs} - \varphi \times df_{rs})\frac{Sat}{df_{rs}} \quad (5)$$

where Sat reflects the satisfaction value. The distance factor
joining the link between sensor r and s is given by the following Eq.(6).

$$df_{rs} = \sqrt{\frac{df_{rs}}{L(S_k)(L(S_k) - d_{rs} + 1}} \quad (6)$$

IX. CONCLUSION

This paper analyzes and compares challenges in wireless sensor network, overview of WSN architecture, some existing trust models available in WSN and then elaborates ant colony optimization algorithm. Using ant colony optimization algorithm provide trust and reputation management in wireless sensor networks. This BTRM-WSN system based on ACO compared to existing TRMs successfully increases the accuracy in finding trustworthy sensors and level of security.

REFERENCES

[1] J. P. Walters, Liang, Z. W. Shi and V. Chaudhary., "Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing", Y. Xiao, Ed.: Auerbach Publications, CRC Press, 2006.

[2] Y. Wang, G. Attebury and B. Ramamurthy., "A Survey of Security Issues in Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, vol. 8, pp. 2-23, 2006.

[3] Xu Wu, "A Lightweight Trust Establishment Method for Wireless Sensor Networks", AISS:Advances in Information Sciences and Service Sciences, Vol. 3, No. 9, pp. 147 ~ 152, 2011.

[4] T. Zia and A. Zomaya., "Security Issues in Wireless Sensor Networks", International conference on Systems and Networks Communication (ICSNC '06), , Tahiti, French Polynesia 2006.

[5] Marmol F.G., Perez G.M., "Providing Trust in wireless sensor networks using a bio-inspired technique", Telecommunication Systems, Volume 46, Number 2 (2011) , pp.163-180.

[6] Momani M, Challa S. Survey of trust models in different network domains. International Journal of Ad hoc Sensor and Ubiquitous Computing (IJASUC) 2010; 1(3):1–19.

[7] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E.A survey on sensor networks. IEEE Communications Magazine 2002; 40(8):104–112.

[8]Mármol, F. G. and G. M. Pérez. "Providing Trust in Wireless Sensor Networks Using a Bio-Inspired Technique." Telecommunication Systems 46.2 (2011): 163-180.

[9] Dorigo, M., M. Birattari and T. Stutzle. "Ant Colony Optimization." Computational Intelligence Magazine, IEEE 1.4(2006): 28-39.

[10] Mármol, F. G. and G. M. Pérez. "TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks." Communications, 2009. ICC '09. IEEE International Conference on. Dresden: IEEE, 2009. 1-5.

[11] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in Proc. Second IEEEWorkshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22.

[12] F. Bao, I. Chen,M.Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and itsapplications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manag., vol. 9,no. 2, pp. 169–183, Jun. 2012.

[13] Srinivasan, A., et al. "Reputation and Trust-based Systems for Ad Hoc and Sensor Networks." On Trust Establishment in Mobile Ad-Hoc Networks. Ed. A. Boukerche. Wiley & Sons, 2007.

[14] Martincic, F. and L. Schwiebert. "Introduction to Wireless Sensor Networking." Handbook of Sensor Networks