Efficient and Secured Ant Routing Algorithm for Wireless Sensor Networks

Benamar Kadri[1], Mohammed Feham[1], and Abdellah Mhammed[2]
(Corresponding author:Benamar Kadri)

STIC Lab., Department of Telecommunications, University of Tlemcen, Tlemcen, Algeria[1]
Telecom Sud Paris, France[2]
(Email: benamarkadri@yahoo.fr)

(Received May. 1, 2012; revised and accepted July 24, 2012)

Abstract

Ant colony based routing algorithms addresses the adaptation of the collective behaviors observed in natural ant colonies for routing in wireless sensor network WSNs, ant swarms usually collectively achieve adaptive, scalable, and robust optimized paths between the net and the source of food with little intelligence and capacities at each individual which is very suitable from WSNs perspective which are composed of small sensors with limited capacities and resources in hostile and unpredictable environment. In this paper, we are going to adapt the conventional ant routing algorithm for WSNs, by taking into consideration their traffic pattern and devices' constraints. The proposed protocol affects the task of route discovery to the base station which periodically launches forward ants over the network to discover routes and inform sensors about its location instead of letting each sensor doing this task individually which consumes sensors' resources and decreases the network lifetime due to the broadcasting nature of the forward ants. We have also proposed to execute a handshake during the route discovery in order to secure links between each sensor and the base station, the use of the underlying routing requests for the handshake has considerably saved sensors' battery power with a good threshold of security. Simulation results in last section show that the proposed solution saves considerably the sensors' battery power and extend the system lifetime compared to the original ant routing algorithm and AODV.

Keywords: AODV, ARA, OARA, routing, security, WSNs

1 Introduction

Wireless sensor networks WSNs are composed of hundreds to thousands of small, low cost, low power and multifunctional sensor nodes, having the possibility to sense environment measures like temperature, pressure and movement to allow environment monitoring [2], due to their flexibility, facility of deployment and their costless WSNs known several fields of application ranging from military applications for battlefield surveillance to environment and habitat monitoring [4].

Routing in conventional wireless networks stays a challenging task due to ad hoc paradigm of these networks as well as the nature of the used medium; nevertheless routing in WSNs is more difficult due to sensors' constraints, applications specifications and the nature of environment which is unpredictable and hostile. In literature routing in WSNs was treated in several ways and techniques by adapting the existed conventional routing protocols for the context and the specificities of this kind of networks, such as the nature of devices, environment and applications.

Ant colony routing algorithms are the most promising protocols for WSNs regarding their criteria which are very suitable for WSNs, since ants in nature are small insects with limited capacities and intelligence trying to find and optimize path between the source of food and the nest, which is comparable to WSNs usually composed of constrained tiny sensors equipped with little memory, limited and non-rechargeable battery, less powered processors, and small bandwidth links in an unpredictable and hostile environment [3].

In literature ant routing was developed for conventional wireless network, having different needs and characteristics compared to WSNs. Therefore, in this paper we are going to present and adaptation of ant routing algorithm for WSNs which take into consideration the traffic pattern of WSNs usually in the form of many to one, our proposed algorithm limits the task of route discovery to the base station instead of doing this by each sensor over the network which is not efficient and consumes the network resources. We have also proposed to execute a handshake during the route discovery phase destined to establish a symmetric encrypting key used for encrypting traffic between the base station and sensors over the network.

2 Routing in Wireless Networks

Several classifications of routing algorithms in wireless ad hoc network exist towards the specificities of wireless

networks such as node mobility, devices' constraints as well as the underlying technology:

1) **Proactive protocols:** Also called table driven protocols, this category of routing is inspired from conventional routing, in which the whole topology of the network is kept by each node over the network in its routing table. Node mobility and topology changing are treated by periodic routing tables exchange or hello messages. Routes are found immediately however the maintenance of the routing tables consumes the network resources due to the overhead imposed by routing table update; this category of routing is not practice for WSNs, since the existed memory at each sensor does not support the increasing number of entries in the routing tables [3].

2) **Reactive protocols:** The shortcoming of proactive routing is the increasing size of the routing tables since wireless nodes can't keep the whole topology of the network in their routing tables especially in WSNs, the reactive routing protocols propose to find routes on demand. In the way that, whenever a node needs to establish a route to a given destination it diffuses a route request which is propagated over the whole network until it arrives to the destination node which responses by a route reply to establish the final route between the source and the destination nodes. This kind of routing is very suitable for wireless networks however there is an additional overhead during the route discovery due to flooding used for route request broadcasting [3].

3) **Hierarchical routing:** Also called hybrid routing, these protocols try to overcome the shortcoming of reactive and proactive protocols by using a combination of the two strategies. The hybrid protocols divide the whole network into regions or clusters and use a proactive technique inside the cluster and a reactive technique outside the cluster, in the way that the network topology is kept for close neighbors and routes to far nodes, are established using a route request launched by the cluster head using a reactive strategy, which minimize considerably the overhead of routing [20].

4) **Swarm intelligence based routing:** This category of routing is recently developed for wireless networks; it is inspired from insect communities such as ants and honey bees which very often collectively execute smart actions with only a little intelligence and capabilities at each insect. This aspect is very practice from the wireless ad hoc networks perspective since each node within an ad hoc network can be viewed as an ant in a hostile and unpredictable environment with limited capabilities trying to find its way to food or to the nest. Using the same idea, sensors launch artificial ants to discover all possible routes to the base station, like real ants the artificial ones use artificial pheromone to compute probability and decide the next hop [7].

5) **Geographical routing:** This kind of routing is based on the position of nodes; node location can be specified geographically using a GPS (global position system) or relatively according to a fixed station. Paths between two nodes are chosen according to the real distance between the source and the destination computed using the geographical coordinates of nodes. This kind of routing can be applied to all the routing algorithms defined above by adding node position as criterion for choosing the best route which has the shortest distance rather than the one having the minimum of hops which can be very practice for WSNs where the position of sensors is used for many objectives [1].

6) **Energy efficient routing**: these protocols are developed for constrained wireless networks composed of small and constrained devices such as sensors and handled devices in mobile ad hoc networks (MANETs), the idea behind these protocols is to include the aspect of energy in route selection by choosing nodes with more battery power for routing in order to guaranty the continuation of service under battery power constraints which is the case in the majority of wireless devices which may save the battery power of nodes and extends the network lifetime[15].

7) **Quality of service based routing:** future WSNs will need more bandwidth, especially those network destined for video surveillance, therefore the QoS routing are developed in order to include the aspect of QoS in routing since all the developed routing protocols in literature do not consider this aspect. QoS routing uses the link quality and available nodes' resources as parameter for route selection in order to guaranty the needed QoS [1].

8) **Secure routing:** regarding the nature of the used medium, devices constraint and the nature of the environment of deployment very often hostile and unpredictable, a wireless network is usually exposed to several risks and attacks. Therefore developing secured routing is a persistent need to avoid the increasing number of attacks. This category of routing tries to implement key distribution and management to establish encrypting keys used by the network nodes to ensure data confidentiality and authenticity [12].

3 Routing Challenges and Objectives

As described above WSNs are usually composed of sensors having reduced computing, radio and battery resources as well as the ad hoc paradigm of wireless sensor networks relying on multi hop to ensure connectivity over the network without any infrastructure or centralized authority any protocol should take into consideration the following characteristics of a WSN [10,17,21]:

1) **Constrained Devices:** Due to their size sensors are extremely limited in resources (battery power, computing power, storage capacities) which make the development of applications and protocols for WSNs a challenging task. Therefore the developed protocols and services for WSNs must take these constraints during development by developing efficient and robust security or routing

protocols which minimizes the number of operations needed for executing any task.

2) **Traffic pattern:** as described above a WSN is deployed in a large region destined to surveillance or remote controlling where a set of sensors collect environment measures and send them to a sink node or a base station. Thus, the traffic pattern is many to one in the way that all sensors get environment measures and sends them to the base station. Accordingly, the routing protocol must take into consideration this pattern of traffic to manage route establishment and maintenance.

3) **High number of sensors:** Future WSNs will be composed of hundreds to thousands of sensors geographically dispersed in a large area, with limited resources. Therefore any developed protocol must allow the network scaling with the same performance for all sizes of the network.

4) **Absence of infrastructure:** Although a WSN is composed of sensor nodes wirelessly linked to each other, responsible of establishing, maintaining and securing the connectivity with the base station without any administrative authority or fixed routers. Thus sensors collaborate in a distributed fashion to manage the network security and routing.

5) **The nature of environment**: Generally, a wireless sensor networks are intended for remote controlling and surveillance, deployed in unpredictable and hostile environment, making them subject of many risks such as failure and attacks. Therefore, the routing service continuation after any incidence such as attacks and environment changing must be guaranteed

6) **Security:** usually deployed in hostile environments such as battlefields in addition to the nature of medium which is opened to each one with the adequate hardware and software, WSNs are subject of many attacks ranging from simple eavesdropping, denial of service and routing attacks to physical attacks. It seems that the security service must be natively implemented in routing to guaranty the security of the exchanged data and resist against attacks.

4 Swarm Intelligence Routing

4.1 Ant Colony Heuristics

An ant colony is composed of millions of ants usually well organized and structured; individually ants are incapable to perform structured tasks, however due to their social nature, ants can achieve complex tasks such as build and protect their nest, carry large items, find and optimize routes between their nest and the source of food. Communication between ants is based on a chemical substance called pheromone. During its movement each ant deposits a certain amount of pheromone on its trail; this pheromone helps it to find its way back to the nest. The Pheromone deposed on its trail is also detected by other ants within the same colony which leads to an implicit way of communication between ants which is used by the whole colony to organize, optimize and structure their movement in a large and unpredictable area. Ants are attracted by the pheromone concentration which always leads to the recent trail and therefore to the shortest path to food or nest [7].

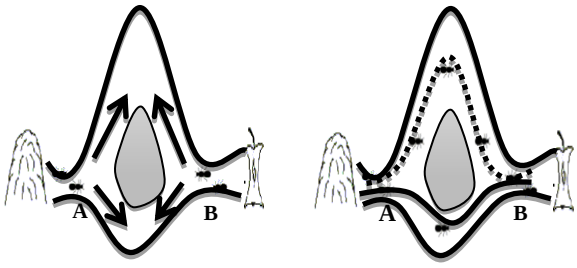

Figure 1: path shortening in real ants' colony

While looking for food an ant deposits pheromone on its trail, this pheromone is used by the same ant to find path to its nest, other ants can also smell pheromone which leads them to the source of food. Experiment shows that ants follow the high concentration of pheromone which leads them to the most recently used paths which leads to shorten the paths between the source of food and the nest.

The principle of finding the shortest path can be explained using the case of figure 1. Whenever an ant arrives to the junction A near the nest for the first time it chooses one of the two paths, however due to time the concentration of pheromone in the upper and the lower path evaporates. However the concentration of pheromone in the lower path will be more than in the upper path, since ants going cross the lower path arrive faster to the junction B. Over time each new coming ant to the junction A or B will choose the lower path having the higher pheromone concentration which leads to choose the shortest path.

4.2 Ant Routing Algorithm

As devoted in the previous section, ants can find, maintain and optimize their trail between the source of food and the nest using little intelligence and communication capabilities by each individual in the colony.

From WSNs perspectives, it seems that the characteristics of such communities are very suitable to ensure routing, since a WSN is very often composed of small sensor nodes with limited capabilities working together to ensure the objectives of the network as well as the connectivity of the network and the continuity of the routing service.

Inspired from real ants the ant routing algorithm ARA [8] uses artificial ants and pheromone to discover and optimize route from a given source node S to a destination node D in a WSN. Generally, ARA uses two kinds of artificial ants for route discovery and establishment:

Forward ant (FANT): forward agent is used to discover routes from the source to the destination node. This agent

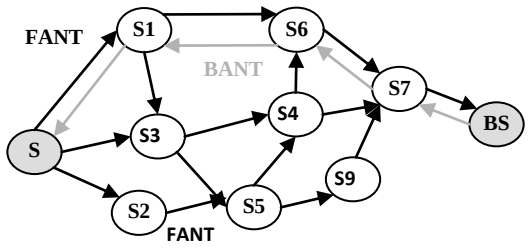

Figure 2: Forward and backward ants in ARA

travels over the entire network in order to find all possible route from S to D, similar to the discoverer ants in real ant colony which go far in the nature in order to find any possible source of food, during her trip over the network each ant deposit a constant amount of artificial pheromone used after by intermediate nodes in order to shorten paths.

Backward ants (BANT): This kind of ants follows the same path established by the FANTs in order to establish the final route from S to D in order to inform S about all the possible routes.

During their lifetime the BANT and the FANT modify at each hop the artificial pheromone for each edge over the network by adding a constant amount of pheromone $\Delta\varphi$ at each visit to any intermediate node emulating real ants. Consequently, ARA uses a pheromone table in which it saves the level of pheromone for each edge. So, each node has a record in this table for each edge, the pheromone table is increased by FANT and BANT and accordingly decreased due to time.

Using the value of pheromone for each edge, each node computes the probability to use one of these edges for routing using the following equation:

$$p_{i,j} = \begin{cases} \dfrac{\varphi_{i,j}}{\sum_{j \in N_i} \varphi_{i,j}} & j \in N_i \\ 0 & j \notin N_i \end{cases} \qquad (1)$$

$$\sum_{j \in N_i} p_{i,j} = 1$$

4.3 Previous Work

Since the first use of Ant colony optimization for routing in ad hoc networks, several algorithms and adaptations exist in literature to adapt this heuristic for wireless networks:

1) ***Position Based Ant Colony Routing Algorithm for Mobile Ad-hoc Networks:*** the authors in this algorithm [13] combine the idea of ant colony optimization with geographical coordinate of the wireless nodes. Using a reactive strategy POSANT establish routes only when there is a collection of data packets need to be sent. Information about the position of nodes is used as a heuristic value for finding the next hop over the network. POSANT is able to find optimum or nearly optimum routes when a given network contains nodes of different transmission ranges.

2) ***QoS-aware Ant Routing with Colored Pheromones:*** this protocol is proposed for Wireless Mesh Networks, this protocol [9] is an ant-based algorithm that takes the required Quality of Service (QoS) into account by using different colors of pheromone for different classes of traffic. The different colors are aligned to four traffic classes which differ in provided bandwidth, delay, and jitter. Thus, the algorithm finds network routes providing a QoS specific to the particular application requirements, which enables better overall network efficiency for a system of applications with heterogeneous QoS requirements.

3) ***Link quality based ARA***: due some design limitations in the basic Ant routing algorithm, since it do not gives the necessary consideration to the ad hoc networks characteristics in the process of pheromone update and route selection. LQARA [11] tries to improve the Ant Routing Algorithm by defining a new mechanism of pheromone computing based on the link quality. The link quality between two neighbors can be affected by many parameters such as distance, battery power and mobility, which makes it more promising as a parameter for route selection. In addition to link quality LQARA uses the number of connections over the same path as parameter for route selection, in order to choose paths with fewer connections (traffic) as route in order to save resources of intermediate nodes over this path by distributing the network traffic over other nodes and consequently increasing the system lifetime as well as the end to end delay.

4) ***AntNet - Distributed Stigmergetic Control for Communications Networks:*** The idea in AntNet is to use two agents for discovering and establishing routes over the network (forward and backward ants) [18]. These agents collect information about delay, congestion status and the followed path in the network which are used for route selection. Forward ants are emitted periodically from each node to a randomly selected destination. This transmission occurs asynchronously and concurrently with the data traffic. As soon as a forward ant arrives at the destination, a backward ant moves back to the source node reverse the path taken by the forward ant. The backward ants get their information from the forward ants and use it to achieve routing updates at the nodes. Therefore, each node over the network has in its routing tables the next hop of the path leading to any destination over the network.

5) ***Ant based Self-organized Routing Protocol for Wireless Sensor Networks:*** this protocol [6] is an improvement of ant routing for wireless sensor networks, which is based on delay and energy. The used factors help WSN in improving the overall data throughput; especially in case of real time traffic while minimizing the energy consumption. The algorithm is also capable to avoid routing loops. Simulation results given by the authors

have proven the efficiency and feasibility of the proposed enhancement of ARA for WSN.

4.4 Discussion

As described above several ant routing algorithm were proposed for wireless networks, trying to adapt and improve the strategy of ant colony heuristic for the specificities of mobile networks such as devices' constraints, radio medium as well as the nature of environment. However the majority of the proposed adaptations are useless for wireless sensor networks which are characterized by a very constrained devices, limited bandwidth and having different needs and traffic pattern compared to the conventional wireless networks.

Therefore, any adaptation of ant colony heuristic for WSN must take into consideration the traffic pattern of WSN which is in the form of many to one in order to save the network resources and improve the network performance. In the other hands the proposed solution must implement a security mechanism in order to resist against attacks which are more frequent in WSN compared to conventional wireless networks, since a WSN is very often part of a hostile environment exposed to numerous attacks such as spoofing, eavesdropping and physical attacks.

5 Optimized ARA for WSNs

In WSNs the traffic pattern is many to one where sensor nodes get environment measures and sends them to a sink node or a base station. Therefore, using the conventional ant routing algorithm to establish routes between each sensor and the base station is not efficient, because sending of a FANT by each sensor overheads the network and consumes sensors' battery power and decreases the network lifetime since the FANT is propagated using flooding.

Thus, we propose to affect the task of route discovery to the base station which periodically sends a FANT to all sensors over the network in order to inform sensors in the network about the path to the base station rather than waiting for the FANT from each sensor which is very costly regarding the energy and the bandwidth consumed during the FANT propagation, especially when we take into consideration the increasing number of sensors.

In this paradigm of ant routing algorithms we anticipate the possibility that each sensor sends a FANT to establish a route with the base station by launching this operation by the base station. The period of the FANT is fixed according to period used by sensors for sending environment measures to the base station in order to ensure the availability of routes

5.1 Forward Ant (FANT)

Like the conventional ant colony routing algorithm the forward ant is sent in order to discover all possible routes

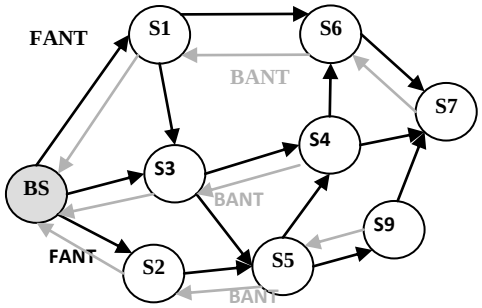

Figure 3: Forward and backward ants in OARA

between the base station and each sensor over the network. The FANT is propagated over the entire network and visit each sensor in the network, like real ants at each visit to an intermediate node it increases the local value of pheromone with $\Delta\varphi$.

In our proposed improvement of ant colony routing we propose to affect the task of sending FANTs to the base station, this FANT is destined to inform sensors over the network about the location of the base station, therefore each sensor over the network learns the path which leads to the base station and rebroadcast the FANT.

In order to avoid routing loops and the network resources wasting the FANT is treated once by each sensor using a unique sequence number affected to each new FANT, therefore each sensor when receives a FANT it verifies the sequence number has been already treated or not, if the FANT was not treated it is propagated over the network until it arrives to the edge of the network, otherwise it is ignored.

5.2 Backward Ant (BANT)

In conventional ARA the BANT is sent by the destination node over the reversed path taken by the FANT in order to establish the final route between the source and the destination node. Like the FANT the BANT modifies the value of pheromone by adding a constant amount of pheromone $\Delta\varphi$ at each intermediate node. In optimized ARA the BANT is sent by each sensor after receiving a FANT coming from the base station after a predefined delay in order to avoid network congestion. Each intermediate node decides the next hop for the BANT according to the value of probability computed using artificial pheromone using the Equation (1).

5.3 Route Maintenance

After the establishment of the final route using the route discovery mechanism described above, this route is used by the source and the destination nodes as long as there is no link failure over this route, however whenever an intermediate node loses the connectivity with its next hop due to link failure an error packet is sent to the source node, the route error packet contains:

- Error Source Address: The address of the node originating the Route Error (node has discovered the link failure).
- Error Destination Address: The address of the node to which the Route Error must be delivered.

This packet is forwarded over the reverse path taken by data packets by each intermediate node which looks if there is any alternative route; otherwise the error packet is forwarded until it arrives to the source node which waits for the next FANT if there is not an alternative route.

5.4 Securing ARA

Security is very important issue in wireless networks, due to the broadcasting nature of the used medium giving the possibility to anyone in the neighborhood of the network to eavesdrop or modify the exchanged data. Hence, the use of security scheme is primordial to protect the exchanged data from outsider attackers.

Consequently we propose to execute a handshake destined to establish a symmetric encrypting key used to encrypt ordinary traffic exchanged with the base station, we propose to use as support for this handshake the BANT sent by sensors to the base station.

In order to make in practice the specifications of our security scheme over ARA we assume that:

- The base station has a pair of keys (private and public key) used to authenticate the base station by sensors.
- Each sensor is capable to use symmetric and asymmetric encryption.
- Each sensor has the capacity to save at least the public key of the base station and a session key used for data encryption.
- Each sensor node gets the public key of the base station before deployment from an off-line dealer.

To establish the encrypting keys between sensor and the base station, each sensor launches the handshake when receive the first FANT, by generating a random symmetric key, encrypts this key by the public key of the base station and sends it included in the BANT.

We propose to encrypt the symmetric key with the public key of the base station in order to guaranty the security of this key since only the base station has the valid private key to decrypt this message which guaranties its confidentiality, integrity and authenticity.

The use of the BANT as support for the handshakes saves sensors' battery power, since each sensor need only to encrypt the symmetric key with the public key of the base station which is not significant regarding the energy consumption.

After the reception of the BANT by the base station it saves all the received encrypting keys in a global table used to identify each sensor and secure communication with that sensor.

In order to enforce security, a proactive key update can be launched periodically by sensors; the key update is executed by executing the same handshake defined above. The period of key update is defined according to the complexity of the used encryption algorithm, the key size and the nature of the environment of deployment.

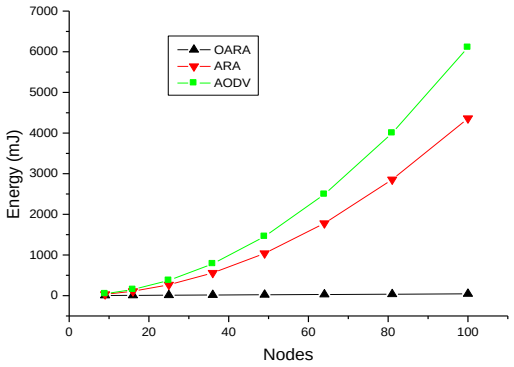

Figure 4: The energy consumption of Route discovery

Using ECC (Elliptic Curve Cryptography) on a Berkeley/Crossbow motes platform Mica2dots [6] consumes 22, 82 mJ with a key size of 160 bits. Therefore, for encrypting the symmetric key of 64 or 128 bits the total energy is around 22,82mJ.

Compared to other schemes in literature [14] it seems that the proposed key distribution scheme is very efficient due to the exploitation of the underlying routing protocol for handling the handshake primitives.

6 Analysis of Optimized ARA

6.1 Energy Consumption

The energy cost of any routing protocol is determined by the energy required for the transmission and the reception of the protocol messages by each sensor such as FANT and BANT.

The total size of FANT and BANT in ARA is around 5 Bytes, using a Berkeley/Crossbow motes platform Mica2dots as platform [13], the transmission of a single byte of data requires 59,2µJ and 28,6µJ for reception. Therefore the transmission and the reception of a BANT or FANT need respectively 296 µJ for transmission and 143 µJ for reception.

In order to test scalability of the OARA, we have varied the network size from 9 to 100 sensors and we have measured the energy consumption required for route discovery in AODV [16], conventional ARA and optimized ARA.

Figure 4 gives the energy consumption of the route discovery in three routing algorithms which are AODV, ARA and OARA, as we can observe ARA give best results compared to AODV regarding the energy consumption due to route discovery, in the other hands OARA gives best energy consumption compared to both AODV and ARA.

Since OARA exploit the traffic pattern of WSNs for route discovery, in the way that each sensor always treats and forwards the same number of FANTs for any size of the network which is not the case of AODV and ARA in which the number of FANTs and route requests increases with the network widening since each sensor launches the route discovery individually which makes it useless for large WSNs. This means that OARA scales efficiently with the network widening due to the mechanism of route discovery which exploit the traffic pattern of WSNs.

6.2 Scalability

This criterion deals with the possibility to keep the same network performance regarding the network overhead and the energy consumption according to the network widening, this is an important issue since future WSNs will increase in size to get thousands of sensors per region, as proven by simulation it seems that the OARA deals efficiently with the network widening, since each sensor treats the same number of FANTs and BANTs for each route discovery which keeps the network performance constant.

6.3 Security

The security of a routing protocol is defined according to its capacity to guaranty the confidentiality of data and the authenticity of the network nodes. In OARA, we have proposed to share a symmetric encrypting key between each sensor and the base station used to encrypt ordinary traffic which guaranties both confidentiality and integrity of data. The authentication of sensors and the base station is guaranteed using public key cryptography, since only the legitimate base station have the valid private key used to decrypt messages sent from sensors and only legitimate sensors have the valid public key preloaded before deployment which guaranties a mutual authentication between sensors and the base station.

7 Conclusion

In this paper we have optimized the ant routing algorithm for WSNs; the proposed optimization takes into consideration the characteristics of the WSNs such as the traffic pattern and devices' constraints. In the proposed protocol we have affected the task of route discovery to the base station which periodically launches FANTs, the FANTs are used by sensors to define the paths to the base station instead of doing this task individually which consumes the network resources and decreases the network lifetime due to broadcasting nature of FANTs. As shown by simulation the proposed OARA saves greatly the network energy and extends the network lifetime compared to the conventional ARA and AODV.

In order to secure the established link with the base station, we have proposed to execute a handshake during the route discovery phase. Therefore, each sensor when receives a FANT, uses the BANT as support to execute a handshake to share a symmetric encrypting key with the base station. In the way that each sensor encrypts using the public key of the base station a random symmetric key and sends it to the base station included in the BANT. Using the BANT as support for the handshake has considerably saved the network resources, since it does not add any overhead for key establishment. The proposed security scheme ensures confidentiality, authentication and integrity of data over the network.

References

[1] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Network*, vol. 3, no. 3, pp. 325-349,2005.

[2] H. Alemdar amd C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2688-2710, 2010.

[3] J. AlKaraki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Communications Magazine*, vol. 11, no. 6, pp. 6-28, 2004.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[5] E. Bonabeau, M. Dorigo, and G. Théraulaz, *Swarm Intelligence: From Natural to Artificial Systems*, Oxford University Press, 1999.

[6] Crossbow Technology Inc., Processor/Radio Modules. http://www.xbow.com/

[7] G. DiCaro, F. Ducatelle, and L. M. Gambardella, "AntHoc-Net: an ant-based hybrid routing algorithm for mobile ad hoc networks," in *Proceedings of the 8th International conference on Parallel Problem Solving from Nature*, pp. 461-470, 2004.

[8] M. Günes et. al, "ARA the ant-colony based routing algorithm for manets," in *Proceedings of the the Workshop on Ad Hoc Networks (IWAHN 2002)*, pp. 79-85, IEEE Computer Society Press, 2002.

[9] E. Ghasemkhani, R. Alizadeh, and A. M. N. Kousari, "Utilizing colored pheromones and helping ants for wireless mesh networks routing," *Communications and Network*, vol. 4, no. 1, pp. 8-17, 2012.

[10] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Transactions on Industrial Electronics, vol. 57, no. 10, pp. 3557-3564, 2010.

[11] B. Kadri, D. Moussaoui, and M. Feham, "Link quality based ant routing algorithm for MANETs (LQARA)," in *Proceedings of the 12 th Post Graduate Network Symposium*, pp. 218-223, 2011.

[12] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113-127, 2003.

[13] S. Kamali and J. Opatrny, "A position based ant colony routing algorithm for mobile ad-hoc networks," *Journal of networks*, vol. 3, no. 4, pp. 31-41, 2008.

[14] J. C. Lee, V. C. M. Leung, K. H. Wong, J. Cao, and H. C. B. Chan, "Key management issues in wireless sensor networks: current proposals and future developments," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 76-84, 2007.

[15] M. Liu, J. Cao, G. Chen, and X. Wang, "An energy-aware routing protocol in wireless sensor networks," *Sensors*, vol. 9, pp. 445-462, 2009.

[16] C. Perkins and al., *Ad hoc On-Demand Distance Vector (AODV) Routing*, Internet Draft draftietfmanet-aodv-11.txt, 2002.

[17] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.

[18] M. Saleem, G. A. D. Caro, and M. Farooq, "Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions," *Information Sciences*, vol. 181, no. 20, pp. 4597-4624, 2011.

[19] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, and R. RAshid, "Ant based self-organized routing protocol for wireless sensor networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 1, no. 2, pp. 42-46, 2009.

[20] S. K. Singh, M. P. Singh, and D. K. Singh, "A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks," *International Journal of Advanced Networking and Application (IJANA)*, vol. 2, no. 2, pp. 570-580, 2010.

[21] J. Zheng and A. Jamalipour, *Wireless Sensor Networks: A Networking Perspective*, John Wiley & Sons, 2009.

Benamar Kadri is an associate professor in wireless network security, received his engineer degree in computer science in 2004, and his M.S. degree in 2006 from the University of Tlemcen, Algeria. Finished his PhD in wireless ad hoc networks security and routing in 2010. Member of STIC laboratory in the University of Tlemcen, his recent work is dealing with mobile wireless networks, their security, routing and management.

Mohammed Feham received his PhD in Engineering in optical and microwave communications from the university of Limoges, France in 1987, and his PhD in science from the university of Tlemcen, Algeria in 1996. Since 1987 he has been assistant professor and professor of microwave and communication engineering his research interest is in telecommunication systems and mobile networks.

Abdallah Mhammed Associate professor in Network security and dependability. He received his Doctor degree in dependability studies from the Technological University of Compiegne, France. In 1990 he joined the National Institute of Telecommunications, in Evry France. His current teaching activities are dealing with network security services, cryptographic protocols and access controls. Member of the Handicom laboratory, his recent research activities are focused on authentication protocols and architectures, security and privacy in smart environments.