

Secured and Optimized AODV for Wireless Sensor Networks

Benamar KADRI¹, Mohammed FEHAM¹, AbdellahMHAMMED²

¹STIC Lab., Department of Telecommunications, University of Tlemcen, Tlemcen, Algeria

²Telecom Sud Paris, France

E-mail: benamarkadri@yahoo.fr

Abstract— Similar to conventional wireless networks, WSNs are based on multi hop routing to ensure connectivity and data forwarding which makes the routing service a challenging task due to the nature of sensors usually limited in memory, battery and computing capacities as well as the nature of the environment which is hostile and unpredictable making the routing protocols developed for conventional wireless network useless for WSNs without modifications and adaptations for the new context of WSNs. Thus in this paper we present an optimized version of AODV protocol for WSNs which takes into consideration the traffic pattern of WSNs and sensors' constraints. In the proposed protocol we affect the task of route discovery to the base station which periodically informs sensors about its location instead of letting this task to sensors which consumes the network resources due to the broadcasting nature of the route discovery. We have also proposed a key distribution scheme destined to establish a symmetric encrypting key between each sensor and the base station, the proposed key management scheme uses the underlying routing requests to execute handshakes and key update which have greatly saved the network resources and ensured a good threshold of security.

Index Terms— Security, Routing, WSNs, AODV, OAODV, SAODV

I. Introduction

The recent development in microelectronics and embedded systems allows the development 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, these sensors networked using wireless medium form a wireless sensor network WSN, usually composed of hundreds to thousands of sensors that collect application specific data and sends it to a base station relying on multi hop routing [1]. WSNs known several fields of application ranging from military applications for battlefield surveillance to environment and habitat monitoring [2].

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 in WSNs it becomes more challenging due to sensors' constraints and the nature of environment which is unpredictable and hostile.

In this paper we are going to present and adaptation of AODV [3] for WSNs which takes into consideration the traffic pattern of WSNs, nature of the medium and bandwidth constraints...etc, our proposed algorithm affects 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. Therefore, periodically the base station launches route request in order to inform sensors over the network about its location, this route request is used by every sensor over the network to define the path to the base station. We have also proposed to execute a handshake over the route discovery to establish a symmetric encrypting key between sensors and the base station; the handshake uses the route reply as support for key establishment which saves considerably the network resources.

II. Routing in Wireless Networks

Several classifications of routing algorithms in wireless ad hoc network exist toward the specificities of wireless networks such as node mobility, devices' constraints and the application of the network. According to the architecture of the network flat or hierarchical, the used strategy [4](reactive or proactive) or the underlying technology the following classifications exist:

2.1 Proactive protocols: these routing algorithms such as OLSR (Optimized Link State Routing)[5] and DSDV (Dynamic Destination- Sequenced Distance-Vector)[6] are inspired from the wired routing in the way that each node over an ad hoc network saves the whole topology of the network in its routing table. Node mobility and topology changing are treated by periodic hello messages. Routes are found immediately however the maintenance of the routing tables consumes the network resources.

2.2 Reactive protocols: The reactive routing protocols such as DSR (dynamic source routing)[7] and AODV (ad hoc on demand distance vector) [3] find routes on demand. In the way that each node launches route discovery to find routes to a given destination by diffusing a route request; this route request is propagated over the network until it arrives to the destination node which responds by a route reply to establish the final route between the source and the destination node.

2.3 Hierarchical routing: Also called hybrid protocols, these 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 the rest of routes are established using a reactive strategy, which minimizes considerably the overhead of routing. For WSNs, hierarchical routing is very efficient for data aggregation since the cluster head play the role of the aggregator which minimizes considerably the overhead and the energy consumption due to forwarding redundant data [8]

2.4 Geographic routing: This kind of routing is based on the position of nodes 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 [9]

2.5 Other classification: due to the diversity of wireless networks and their applications, other adaptations and optimizations derived from the classifications defined above exist trying to include the specificity of nodes and the network such as energy, quality of service and security:

- **Energy efficient routing:** these protocols are developed for both mobile ad hoc networks (MANETs) and WSNs in order to include the aspect of energy in route selection by choosing nodes with more battery power for routing to guaranty the continuation of service for long time. Using the energy as a parameter for routing may save the battery power of nodes and extends the network lifetime especially for WSNs which are deployed for long period without power splay [10].
- **The quality of service based routing:** future applications developed for WSNs especially the video surveillance will need more bandwidth; therefore the QoS routing protocols implements the aspect of QoS by including in route selection the criteria of QoS such as the link quality and nodes' resources in order to reserve the best path for traffic forwarding[11].

- **Secured routing:** regarding the nature of the used medium, a wireless network is open to anyone with the adequate hardware and software. Therefore developing secured routing is a persistent need to avoid the increasing number of attacks against WSNs. Many extensions are given in literature to secure routing over wireless networks[12]

III. Routing Challenges and Objectives

As described above WSNs have many features that distinguish them from conventional wireless networks, WSNs are usually composed of constrained tiny sensors equipped with little memory, limited non-rechargeable battery, less powered processors, and small bandwidth links. As well as the ad hoc paradigm of WSNs relying on multi hop to ensure connectivity over the network without any infrastructure or centralized authority, therefore any protocol developed for WSNs should take into consideration the following characteristics:

3.1 Traffic pattern: due to their field of applications destined for remote monitoring and surveillance, communication in WSNs is based on event-driven, query driven, continuous monitoring, or a combination of these schemes of communication. The traffic pattern is usually many to one in the way that all sensors get environment measures and send them to a sink node or a base station. Accordingly, the routing protocols must take into consideration this pattern of traffic and manage route establishment and maintenance under the considerations of this traffic pattern [13].

3.2 Constrained Devices: Due to their size, sensors are extremely limited in resources (battery power, computing power, storage capacities) which make the development of routing and security protocols for WSNs a challenging task. For example, in proactive routing protocol the available memory in sensor nodes cannot keep the whole network topology in their routing table, the same thing for reactive protocols usually based on flooding to establish routes over a network which consumes sensors' battery power. Therefore the conventional routing protocols developed for conventional ad hoc networks are useless without the adaptation for the WSNs context by taking into consideration the sensors' constraints [14].

3.3 Energy efficiency: Sensor nodes are equipped with small non-rechargeable batteries. Therefore, the minimization and optimization of the number of operations by any protocol is crucial to extend the sensor battery and therefore the network lifetime. Consequently, routing protocols must minimize (i) the transmission overhead, (ii) the number of operations needed for treating each routing packet, (iii) memory space used by routing tables. In the other hands routing protocol must equilibrate the use of intermediate node for data forwarding in order to extend the whole network lifetime and speed up data forwarding [14].

3.4 Scalability: this criterion deals with the network widening, because future WSNs will be composed of hundreds to thousands of sensors geographically dispersed in a large area. Therefore the developed protocol must allow the network scaling with the same performance regarding communication and treatment overhead under all possible topologies with any number of sensors [14].

3.5 Security: the aspect of security is very important when designing any routing protocol especially the wireless ones due to the nature of the used medium naturally opened within the area of deployment. Very often deployed in a hostile environment; WSNs are subject of many attacks. Therefore, routing protocol must implement natively the aspect of security in order to ensure the confidentiality and the integrity of data as well as the authentication of sensors [15].

IV. AODV

In this section we are going to present the Ad-Hoc On-Demand Distance Vector (AODV)[3], AODV was developed for conventional mobile ad hoc networks MANETs. AODV can be viewed as a combination of a reactive routing protocol in the sense that it establishes routes on demand using route discovery requests, in the other hands it uses routing tables and hello messages to save and update paths and ensure neighbors connectivity.

Mainly AODV is inspired from two routing protocols which are the dynamic source routing DSR and DSDV, in the way that it uses the strategy of DSR for establishing routes using the route discovery and maintenance requests and it partially uses the structure of routing table of DSDV and the hello messages for updating these tables, nevertheless the hello messages are diffused in one hop neighborhood.

4.1 Route Discovery

The route discovery mechanism is intended to establish a route between two nodes which are not in the transmission range of each other and have not a path in their routing tables. Therefore the source node launches a route discovery as follow:

It creates a route request to discover all possible routes leading to the desired destination. The route request contains the addresses of the destination and the source node, a sequence number to indicate the freshness of the route as well as the number of hops initiated to 0 which is used as metric for route evaluation.

TYPE	SRC	DEST	PRV	SEQ	HOP	TTL
------	-----	------	-----	-----	-----	-----

Fig. 1: Structure of packets in AODV

- TYPE: type of the packet (RREQ, RREP, RRER, DATA).
- SRC: source node.
- DEST: destination node.
- PRV: the previous hop.
- SEQ: sequence number.
- HOP: hop count.
- TTL: time to live.

Each node over the network when receives this RREQ, it verifies if it has been already treated by verifying its sequence number. The Sequence Number in the RREQ is used by intermediate nodes to insure that they do not rebroadcast the same RREQ several times which consumes network resources and causes routing loops. Thus according to the sequence number intermediate nodes decide to ignore the RREQ or rebroadcast it to their neighbors after the modification of the HOP, PRV, TTL fields to the new values.

The same procedure is executed by each node over the network until the route request arrives to its destination, which generates a route reply (RREP) and sends it back to the source of the RREQ. The RREP contains the sequence number of the established route, the addresses of the destination and the source node.

Each intermediate node that receives the RREP, increments the hop-count in the RREP gets the next hop to the source node from its routing table; the RREP is forwarded in the same way by each until it arrives to the source node.

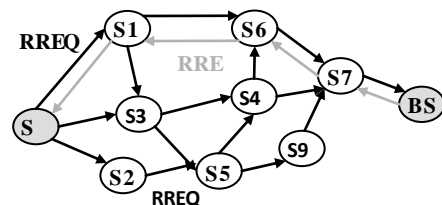


Fig. 2: Route discovery

4.2 Routing Table

Like DSDV, each node over the network uses a routing table for storing routes to each destination over the network; these routes are obtained during the route discovery phase. Consequently, AODV stores in its routing table the next hop to reach each node over the network as well as the number of hops to reach this destination.

In order to avoid routing loops and the enable routes freshness, a sequence number is added to each entry in the routing table, a route with a high sequence number are more desired since they are fresh and reflect the current state of the network. An additional mechanism to ensure route freshness is the route lifetime, if during

this time the route has not been used or updated, the entry is discarded from the routing table.

Routing table			
SEQ	DEST	NEXT	HOP
15	BS	S1	4
20	S7	S1	4
22	S4	S1	4

Fig. 3: Structure of routing table

4.3 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, it generates a Route Error (RERR) message and sends it back to the source nodes via its precursor nodes and marks the entry of the destination in the route table as invalid.

The RERR is forwarded in the same way by each intermediate node until it arrives to the source node which launches a new route discovery to establish a new valid route or uses another route from its routing table if it exists.

4.4 Hello messages

Like proactive routing protocol AODV uses hello messages to update the connectivity with its neighbors, these messages contain the node identifier the current sequence number and a TTL fixed to one, which means that these messages are broadcasted within one hop neighborhood in order to avoid the network overhead. If a node does not receive for each entry in its routing table a hello message, it supposes a link failure with that neighbor and deletes the corresponding entry in the routing table

Hello messages are broadcast if during a given period there is no route discovery to update routing tables and nodes' connectivity.

V. Optimized AODV for WSN

In the conventional AODV routes are established and maintained on the demand of the source node by broadcasting a RREQ in order to discover all possible routes to a given destination, this mechanism is very practice for mobile ad hoc network composed of wireless devices having more resources compared to sensors in WSNs, also the traffic pattern in a MANETs is very often one-to-one in contrary of WSNs which is many-to-one, therefore the specifications of the conventional AODV must be redefined and optimized for WSNs, in order to take into consideration the following characteristics:

- The traffic pattern of WSNs which is in the form of many-to-one.
- Sensors' constraints such as memory and computing power.
- The bandwidth constraints.
- The number of node in the network

Therefore, in the rest of this paper we are going to adapt the conventional AODV for the WSNs context by taking into consideration the characteristics of these networks, we also propose to secure the established links using a symmetric encryption key established during the route discovery phase:

5.1 Route discovery

Taking into consideration the traffic pattern of the WSNs usually many-to-one it seems that each sensor over the network will frequently broadcasts RREQ to establish a path with the base station which overloads the network and degrade its performance especially for large scale WSNs consisting of hundreds to thousands of sensors, to overcome this shortcoming we propose to affect the task of route discovery to the base station. In the way that the base station launches periodically a RREQ over the network destined to inform each sensor over the network about its location. The RREQ is received and rebroadcasted by each sensor over the network, during this period each sensor updates its routing table and adds new routes to its routing table. All entries in the routing tables lead to the base station which is very suitable for WSNs, since only the path to the base station is needed which saves the memory space taken by routing tables.

When receiving a RREQ a sensor verifies if it has already treated this RREQ using the sequence number like conventional AODV, if the RREQ is received for the first time the sensors get from this RREQ the next hop to reach the base station, increment the number of hops in the RREQ and rebroadcast it. Otherwise if the RREQ is already treated it is simply ignored.

After broadcasting the RREQ, the sensor waits a predefined delay to avoid the network blockage and sends back a RREP.

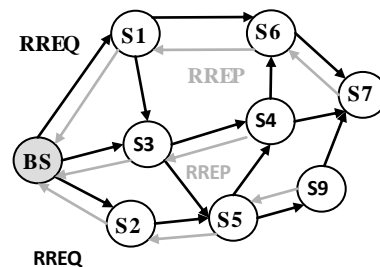


Fig. 4: route discovery in OADV

5.2 Routing Table

Although in WSN the traffic pattern is in the form of many-to-one, in which a set of sensors send periodically environment measures to the base station, therefore each sensor over the network needs permanently one route to the base station which means that the routing table will contain only one or two entries having like final destination the identifier of the base station.

Therefore, OAODV keeps the same structure of the routing table defined in conventional AODV, however only entries to the base station are kept in the routing table which minimize considerably the size of memory space occupied by the routing table. This aspect is much desired from WSNs perspective, since sensors have not the sufficient memory to save big routing tables.

5.3 Hello Messages

Due to the bandwidth constraints as well as the increasing number of nodes in WSNs, diffusing hello messages within a given period overheads the network and wastes sensors' battery power therefore OAODV the hello messages are not used, the connectivity between sensors is guaranteed using the route request sent periodically by the base station which guaranties the update of the routing tables and sensors connectivity.

5.4 Route Maintenance

The route maintenance is treated in the same way like conventional AODV, in the way that the node which detects the link failure sends a RERR message to the source node which waits for the next RREQ broadcasting by the base station in order to get fresh routes. A sensor waits for new RREQ from the base station rather than launching its own RREQ because the RREQs are periodically diffused by the base station. The period of RREQ are fixed by the administrator of the network according to node stability and the environment of deployment.

VI. Analysis of OAODV

6.1 Energy Consumption

The energy cost of any routing protocol is determined by the energy required for the execution of the protocol's primitives such as route discovery and maintenance which is determined by the number and the size of the used requests such as the RREQ, RREP, hello message and RERR. Therefore, the efficiency of the routing protocol is defined according to this criterion which affects the system lifetime.

The total size of an AODV RREQ in both conventional and OAODV is around 7 Bytes, using a Berkeley/Crossbow motes platform Mica2dots as platform [16], the transmission of a single byte of data requires $59,2\mu\text{J}$ and $28,6\mu\text{J}$ for reception. Therefore the

transmission and the reception of a RREQ or RREP need respectively $414,4 \mu\text{J}$ for transmission and $200,2 \mu\text{J}$ for reception.

Four routing table update, conventional AODV uses hello message diffused within one hop having the size 4 bytes which consumes $236,8 \mu\text{J}$ for its transmission and $114,4\mu\text{J}$ for reception.

To test the performance and compare OAODV with conventional AODV we have used as simulation tool TOSSIM. We have varied the number of nodes between 9 nodes to 100 nodes.

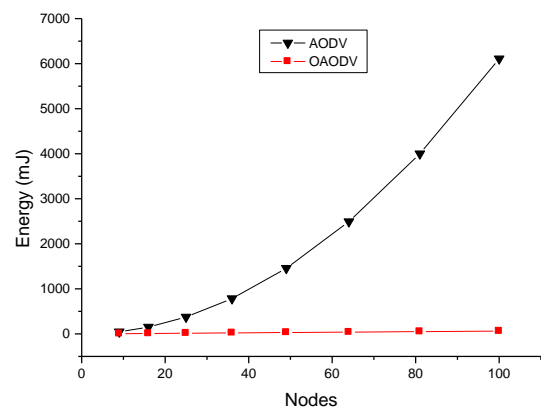


Fig. 5: The energy consumption of Route discovery

Figure 5 gives the energy consumption of the route discovery in both conventional and optimized AODV, as we can observe OAODV always consumes less energy for route discovery compared to the conventional AODV. In the other hands the energy consumption of optimized AODV is stable regarding the network widening, since it consumes approximately the same energy for all sizes of the network however the energy consumption of conventional AODV increases with the network widening which makes it useless for large WSNs.

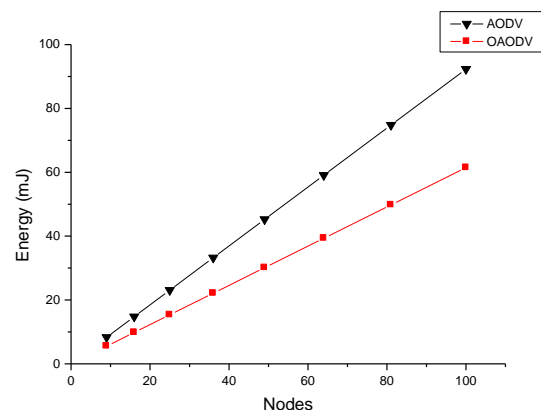


Fig. 6: The energy consumption for Route update

As shown in figure 6 using periodic RREQ launched by the base station to update routing tables and nodes'

connectivity rather than using hello messages is very practice regarding the energy consumption since OAODV consumes always less energy compared to the conventional AODV which consumes more energy to ensure nodes' connectivity and routing table update.

6.2 The network overhead: compared to the conventional AODV, it seems that optimized AODV has decreased the overhead due to routing by decreasing the number of RREQ sent over the network, since the RREQ is broadcasted over the network using flooding which affect greatly the network lifetime. Thus in OAODV the route discovery is done by the base station to limit its effect on the network.

6.3 Scalability: this criterion deals with the network widening, since the WSNs increase in size to get thousands of sensors per region, as proven by simulation it seems that the OAODV deals efficiently with this criterion since the size of the routing table does not increase with the network widening as well as the number of broadcasted RREQ which are the same for all sizes of the network.

6.4 Fault tolerance: this criterion treats the aspect of the maintenance of link failures and topology changing; this aspect is treated by the OAODV protocol using route error messages in order to inform the source node about the link failure.

VII. Securing Optimized AODV

Security is an important issue when designing and deploying any network, especially the wireless ones. Since a wireless network is opened to everyone with the adequate hardware and software making the whole network vulnerable against several attacks ranging from simple eavesdropping to data modification and routing attacks such as sink hole ...etc. Therefore each routing protocol must natively implement security to resist against the increasing number of attacks.

In our optimization of AODV we propose to implement a key distribution scheme using the underlying requests of AODV such as RREQ and RREP. In the way that during the route discovery phase the base station and each sensor over the network cooperate to establish a shared symmetric key used to encrypt the ordinary traffic between them.

Using the RREQ and RREP for key negotiation secured AODV saves the network resources since there is no additional overhead due to security management and key distribution which will greatly save the network resources and decreases the network overhead due to key management schemes.

7.1 Cryptographic Primitives

To make in practice our proposed scheme of security over AODV we propose to use three cryptographic methods in order to ensure the confidentiality,

authentication and the integrity of the data over the network [17]:

- **Symmetric cryptography:** This cryptographic method uses a single key for both encryption and decryption, the used key is shared between the communicating entities using a key management scheme. This encryption method is largely used in conventional networks for data encryption due to its simplicity of use and implementation.
- **Asymmetric cryptography:** Also called public key encryption, this cryptographic method uses two different key for encryption and decryption. One key is kept secretly by its holder and called private key and the second is published for the rest of users in a given community or a network called public key. A message encrypted with public key can only be decrypted with the private which ensures confidentiality, authentication and integrity.
- **Message authentication codes (MACs):** generally, a MAC is used to ensure the integrity and the authentication of messages over networks, the MAC of a packet is obtained by passing the packet into a hash function which results on a digest of a fixed size. This message when encrypted ensures the integrity and the authentication of the exchanged data. For more security and authentication this message can be encrypted using the private key of the source node.

7.2 Network architecture and Assumptions

Due to the traffic pattern of WSNs only the links between the base station and sensors need to be secured to avoid the attack that can be executed against the data sent to the base station, thus each sensor and the base station must share a symmetric key to encrypt the exchanged traffic.

We propose to use Public key cryptography to guaranty the authentication of the base station by giving the base station a pair of asymmetric keys (private, public), the public key is preloaded for each sensor over the network before deployment, this key is used by sensors to authenticate the base station and secure key establishment, which guaranties the integrity and the confidentiality of all dialogues with the base station, since only the base station has the valid private key for decryption.

In order to implement this security scheme we assume that each sensor is capable to use:

- **Asymmetric Cryptography:** To provide authentication of the base station.
- **Symmetric Cryptography:** To ensure the confidentiality of traffic across the network.
- **MAC (message authentication code)** to ensure data integrity.

7.3 Key Establishment

The key establishment is achieved by executing a handshake launched by sensors over the network; this handshake is intended to establish a symmetric encrypting key with the base station. This handshake is executed after the reception of the first route request. The sensor uses the usual route reply RREP sent to the base station as a support for handling the handshake and transporting the encrypting key.

Therefore, each sensor before sending a RREP generates a random symmetric key encrypts this key with the public key of the base station and sends it back to the base station included in the RREP.

The use of the public key for encrypting the key ensures the authentication of the base station, as well as the integrity and the confidentiality of the handshake.

After the reception of the RREP from each sensor, the base station decrypts it using the corresponding private key and stores all the received keys with the identifier of each sensor in a global table used for identifying sensors and managing security over the network.

7.4 System Functioning

After a successful handshake, each sensor shares a symmetric encrypting key with the base station; this key is used to encrypt all traffic exchanged with the base station.

To ensure data integrity, another additional mechanism is used which is a MAC (message authentication code) joined to each message sent to the base station. In the way that each packet is passed in a hash function to obtain a fingerprint encrypted using the shared key. The encrypted MAC is joined to the original packet without any modification on the global structure of the packet.

Another option can be turned on to ensure more security depending on the importance and the nature of the networks is to encryption the MAC joined to each packet using the public key of the base station, this option consumes more energy due to the additional overhead for data encryption however it guaranties a maximum of security.

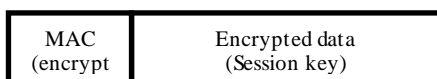


Fig. 6: Packet structure

7.5 Key Update

By nature a wireless sensor network is deployed in a hostile environment or in some area which are not accessible by human, therefore a key update must be executed periodically to enforce security over the

network and avoid long term attack aiming to extract the encrypting keys by analyzing the encrypted traffic over the network for long period.

The key update is achieved using the same mechanism described above, which consists on the generation of a new key after expiration of the period and sends using a RREP as described above.

The period of the key update is defined according to the complexity of the encrypting algorithm and the length of the encrypting key.

7.6 Energy Cost Analysis

In our proposed scheme we use two types of cryptography, symmetric and asymmetric algorithms with an optional use of a hash function as a MAC (message authentication code). We propose to use the ECC (Elliptic Curve Cryptography) as asymmetric algorithm which is more efficient regarding its energy consumption, as a symmetric algorithm we propose the AES (advanced encrypting system) which will be the standardized as encryption system for future networks [17].

The ECC signature and verification applied to Berkeley/Crossbow motes platform Mica2dots [16] 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 22,82 mJ which is the total energy consumed for executing the handshake since there is not any other operations, compared to other schemes in literature [18] it seems that the proposed key distribution scheme is very efficient. This is due to the exploitation of the underlying routing protocol for handling the handshake primitives.

7.7 Security Services

The robustness of a key management scheme is defined according to its capability to guaranty the basic security services [19] which are:

- **Confidentiality:** this aspect ensures that the exchanged data is kept secret from any unauthorized entities over the network. The confidentiality in SAODV is achieved using symmetric encryption enforced using a proactive key update for more security and resistance against long term and cryptanalysis.
- **Authentication:** this aspect deals with the authenticity of the communicating parties over the network. To guaranty this aspect we have used asymmetric encryption in order to authenticate the base station using its public key. In the other hands only legitimate sensors have the valid public key of the base station which is pre-installed in each deployed sensor before deployment.
- **Integrity:** this aspect deals with the possibility to detect data alteration and modification over the

network, to do so we have used a MAC (Message authentication codes) computed and joined to each sent packet between the base station and any sensor over the network, this MAC can be encrypted with the public key of the base station or shared symmetric key.

VIII. Conclusion

In this paper we have optimized AODV for WSNs, in order to take into consideration the traffic pattern of WSN and devices' constraints. In the proposed protocol we have affected the task of route discovery to the base station which periodically launches RREQs over the network, these RREQs are used by sensors to define the paths to the base station instead of letting each sensor launches the RREQs individually which consumes the network resources and decreases the network lifetime due to flooding used for broadcasting RREQs. As shown by simulation the proposed improvement of AODV saves greatly the network energy and extends the network lifetime compared to the conventional AODV.

In the other hands, we have proposed to execute a handshake to share a symmetric encrypting key with the base station used for securing routes with the base station. In order to save the sensors resources and decreases the overhead due to key negotiation we have used the RREP sent by every sensor during the route discovery phase as support for this handshake, in the way that the encrypting key is sent included in the RREP which 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] Hande Alemdar, Cem Ersoy, "Wireless sensor networks for healthcare: A survey", *Computer Networks*, Vol 54, No 15, pp. 2688-2710, 2010.
- [2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey", *Computer Networks*, Vol. 38, No. 4, pp. 393-422, 2002.
- [3] C. Perkins et al., "Ad hoc On-Demand Distance Vector (AODV) Routing," *Internet Draft draftietfmanet-aodv-11.txt*, June 2002.
- [4] Jamal Al-Karaki, and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", *IEEE Communications Magazine*, vol 11, no. 6, pp. 6-28, 2004.
- [5] T. Clausen, and P. Jacquet. "Optimized Link State Routing Protocol (OLSR)". RFC 3626, October 2003, <http://ietf.org/rfc/rfc3626.txt>
- [6] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector (DSDV) for Mobile Computers", *Proc. ACM Conf. Architectures and Protocols (SIGCOMM' 94)*, London, UK, pp. 234-44, 1994.
- [7] D. B. Johnson and D. A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", *IETF Internet draft*, 19 July 2004, <http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt>
- [8] 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. 02, No 02, pp. 570-580, 2010.
- [9] Akkaya, K.; Younis, M. "A Survey on Routing Protocols for Wireless Sensor Networks". *Ad Hoc Network*, Vol 3, No 3, PP 325-349, 2005.
- [10] Ming Liu, Jiannong Cao, Guihai Chen, and Xiaomin Wang, "An Energy-Aware Routing Protocol in Wireless Sensor Networks", *Sensors*, vol. 9, No. 1 pp. 445-462, 2009.
- [11] K. Akkaya and M. Younis, "An Energy-Aware QoS Routing Protocol for Wireless Sensor Networks," in the *Proceedings of the IEEE Workshop on Mobile and Wireless Networks (MWN 2003)*, Providence, Rhode Island, May 2003.
- [12] Karlof, C. & Wagner, D. "Secure routing in wireless sensor networks: attacks and countermeasures". *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113-127, 2003.
- [13] Tilak, S.; Abu-Ghazaleh, N.B.; Heinzelman, W. "A Taxonomy of Wireless Micro-Sensor Network Models". *Mobile Computing Communication Review*, Vol 6, No. 2, pp. 28-36. 2002
- [14] Gungor, V.C.; Bin Lu; Hancke, G.P.; "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid", *Industrial Electronics*, *IEEE Transactions*, Vol. 57 No. 10, pp. 3557 - 3564.
- [15] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.
- [16] Crossbow Technology Inc., *Processor/Radio Modules*, <http://www.xbow.com/>
- [17] Bruce Schneier, "cryptographic appliquée algorithms, protocoles", 2nd edition wiley, 2001.
- [18] Syed Muhammad Khaliq-ur-RahmanRaazi and SungyoungLee. "A Survey on Key Management Strategies for Different Applications of Wireless

Sensor Networks". Journal of Computing Science and Engineering, Vol. 4, No. 1, 2010.

- [19] Wang, Y. ; Attebury, G. & Ramamurthy, B. "A survey of security issues in wireless sensor networks". IEEE Communications Surveys and Tutorials, Vol. 8, N 2, pp. 2-23, 2006.

Authors' Profiles

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 M'hamed is professor in Network security and dependability. He received his Doctor degree in dependability studies from the Technological University of Compiègne, France. In 1990 he joined the National Institute of Telecommunications, in Evry France. Member of the Handicom laboratory, his recent research activities are focused on authentication protocols and architectures, security and privacy in smart environments.

How to cite this paper: Benamar KADRI, Mohammed FEHAM, AbdallahMHAMMED,"Secured and Optimized AODV for Wireless Sensor Networks", International Journal of Information Technology and Computer Science(IJITCS), vol.5, no.6, pp.23-31, 2013. DOI: 10.5815/ijitcs.2013.06.04