International Conference on Wireless and Ubiquitous Systems
8-10 October 2010, Sousse, TUNISIA

SecOPP-A Low-cost Energy Secure Multi-hop Routing Protocol for Wireless Sensor Networks

Abderrahmen Guermazi
CES Research Unit
Higher Institute of technologies studies
Sfax, Tunisia
Abderrahmen.guermazi@isetsf.rnu.tn

Mohamed Abid
CES Research Unit
National School of Engineers
Sfax, Tunisia
Mohamed.abid@enis.rnu.tn

Abstract—**In this paper we are proposing an efficient secure solution to the data centric routing protocol One Phase Pull diffusion which permit multi-hop routing of sensed data. SecOPP provides both Group and Pairwise key distribution with the possibility of rekeying as well as security services: integrity, authentication and confidentiality of exchanged messages. All these are obtained without using a key distribution center or messages adjunction. Security analysis shows that SecOPP protocol can withstand several possible routing attacks in the network. Scalability and low energy consumption are well checked via implementation for TinyOS using NesC and simulated under TOSSIM.**

Keywords-Wireless sensor network, routing protocol, security, tinyos, TOSSIM.

I. INTRODUCTION

Wireless sensor networks (WSN) are often used to monitor a remote environment where many sensor nodes should coordinate to disseminate sensed data towards a sink node. In this context, many routing protocol are proposed to Wireless Sensor Networks (WSNs) [9]. However, there are many attacks against WSNs and especially against routing protocol which are not secure [5]. In this paper, we are interested to secure the One Phase Pull diffusion (OPP) routing protocol [11] used in applications of WSN that need intermittent data sending. OPP is a variant of "directed diffusion"[10] which is a famous data-centric routing protocol based on publish/subscribe communication paradigm[12]. OPP reduces the diffusion overhead in the network to one phase and allows data dissemination through multi-hop routing path.

Security services (Authentication, confidentiality, integrity…) for routing protocol in WSNs are based on both (1) cryptographic algorithms, especially low-cost symmetric algorithms, (2) key distribution schemes. This permits to secure several communication patterns: one-to-all, one-to-some and one-to-one. Several key distribution schemes are proposed in literature [2][3][4]. Most of them cause messages adjunction and more computation to sensor nodes. Knowing that, these are considered as the most expensive operations, in term of energy consumption for constrained resources sensor nodes. As a consequence, this can affect the lifespan of the whole network.

SecOPP protocol requires the design of an appropriate key distribution scheme which satisfies security goals and at the same time causes low storage, computation, communication overhead and energy consumption.

More preciously, SecOPP is expected to guarantee:

- Authentication of interest message broadcasting
- Data message integrity, authentication and confidentiality on multi-hop routing paths.
- Secure distribution of different types of key on multi-hop routing paths
- In-network processing: fusion, suppression…
- Security impact of a compromised node will be limited to its immediate network neighborhood.
- Avoiding of packets injection or replaying older messages
- Efficiency by minimizing energy consumption and reducing communication overhead. So keying mechanism should minimize adjunction of messages and cryptographic algorithms should be lightweight processing.

This paper is organized as follows: section 2 represents the background needed for our work, section 3 illustrates the network organization; section 4 describes SecOPP protocol; section 5 contains a security analysis of SecOPP protocol against the most known routing attacks; section 6 carries out simulations and results; section 7 concludes the paper.

II. BACKGROUND

OPP involves two steps. In the first step, a sink node broadcasts interest messages which are flooded throughout the sensor network. Interest messages support attributes naming which specify a set of constraints to be met by sensed data which sink node expects, like class of data. It is possible to specify other parameters such as the interest expiration period and the sending frequency. In the second step, sources (sensor nodes) with data matching these constraints send data messages back along the best (fastest) gradient from which the first interest message was received. Figure 1 illustrates communication patterns in OPP diffusion routing protocol.

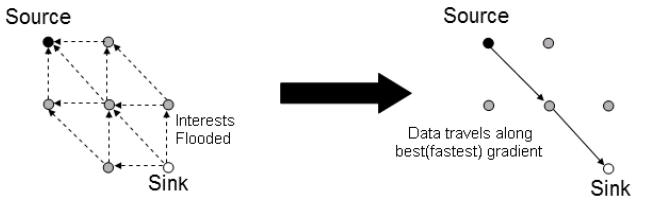

Figure 1. One Phase Pull communication model redrawn from [11]

On the other hand, different key managements for WSNs are proposed in literature:

- Public key schemes: With limited resources, sensor nodes cannot employ sophisticated public key cryptographs. Though, some work on ECC promises easy key management but this is for heterogeneous WSNs where routers dispose most capabilities [6].
- Single network-wide key: a single key is preloaded into all nodes of the network. After deployment, like in Tinysec [7] every node in the network uses this key to encrypt and decrypt messages. The main drawback is that the compromise of a single node causes the compromise of the entire network.
- Complete Pairwise key sharing: For a network of n nodes, (n-1) Pairwise keys are retained in each node's memory. This approach is no scalable.
- Random key pre-distribution scheme: in this scheme, a pool of keys is initially pre-loaded into each sensor. After this, sensor nodes undergo a distributed discovery process to set up shared key for secure communications [8]. This scheme isn't convenient to a centralized bootstrapping communication model like OPP. Also it doesn't ensure that two nodes always are able to compute a Pairwise key.
- Trusted base station: Also called key distribution center (KDC) approach [3] where base station sends the session keys to secure communication between any two nodes. The scheme has small memory requirement. It is resilient to node capture and possible to revoke key pairs. The drawbacks are that the base station must be directly accessible with all the network nodes, so it is not scalable and the base station becomes the attacks target
- Hierarchical key management: It permits in-network processing and supports various secure communication patterns: unicast, multicast and global broadcast. LEAP+ [1] is referred to as the basic scheme of hierarchical key management.

III. NETWORK MODEL

OPP diffusion routing protocol is applied to homogenous WSNs. The number of sensor is about one hundred. All sensor nodes have initially the same capabilities. They are deployed randomly in the field. Density and communication range will permit up to 10 neighbors for each node. On deployment, OPP gives for each sensor node an interest gradient among its immediate neighbors. An interest gradient is a router which belongs to a multi-hop routing path. which permits data dissemination towards sink node. On the other hand OPP gives for each router node a group of sensor members (data gradients). So OPP procure to the deployed WSN a hierarchical organization which illustrated in figure2. This organization makes it possible in-network processing. It results from it a reduction of sending and a reduction of possible collisions on the transmission channel. These aspects lead to save energy by nodes and to increase the lifespan of the network.

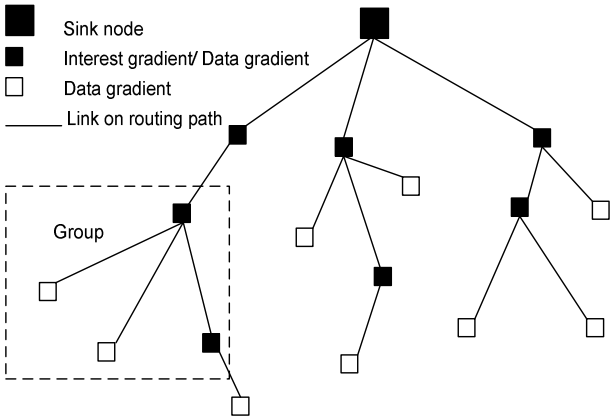

Figure 2. Network organization

IV. DESCRIPTION OF SECOPP PROTOCOL

As we said in III, the deployment of OPP diffusion protocol offers to the WSN a hierarchical organization. Furthermore, to secure different communication patterns in OPP we need to share a Global key, Groups key and Pairwise key. LEAP+ [1] distributes the mentioned keys, but its keying mechanisms are not appropriate to OPP diffusion protocol. In fact, Pairwise key are established in LEAP+[1] with a distributed process. Each node broadcasts a hello message to discover its neighborhood and will establish a Pairwise key with all its neighbors [1]. It isn't the case of OPP where communication is initiated by the sink node. A Pairwise key is needed only between a data gradient and its best interest gradient. Samely, a Group key is only needed to secure multicast between an interest gradient (router) and their data gradients (members). Such hierarchical links are established in OPP where interest messages are broadcast.

Unlike LEAP+[1], in SecOPP Group key must be established before Pairwise key. This will be established in the second step of SecOPP when sensors begin to send data back via their fastest interest gradient.

The following paragraphs describe in detail format of exchanged messages and different operations of SecOPP protocol.

A. Secure broadcast and Group key distribution

The global key is useful to secure broadcast of interest message and to bootstrap other keying mechanism especially Group key distribution. As the same in [1], this key is deleted from each sensor node as soon as the first broadcast of the interest message is completed and Group keys are shared. Global key are loaded to each node before deployment of

WSN. It is the most practical approach. In order to establish Group Keys with a secure manner, we add some fields to the original interest message [11].

The new format of the broadcast secure interest message will be:

$u \rightarrow * : IM \,||\, Nonce \,||\, SecModSub \,||\, KeyTypeSub \,||\, KeyTypeDistSub \,||\, SecModPub \,||\, KeyTypePub \,||\, KeyTypeDistPub \,||\, Enc_{GlobalKey}(GroupKey) \,||\, MAC_{GlobalKey}$

Description and size of added fields are below:

- IM(36bytes): the original interest message of OPP protocol.
- Nonce(2 bytes): sequence number used to determine different subscriptions.
- SecModSub(2flag) : Secure mode subscription specifies the security level for the current subscription (values : Authentication, Authentication-Encryption or Null).
- KeyTypeSub(1flag): Key type used while subscription to obtain service security (values: GlobalKey for the first subscription or GroupKey for next subscription).
- KeyTypeDistSub(1flag): Key type Distributed while Subscription (value: NewGroupKey for first subscription).
- SecModPub(1flag): Secure mode publication specifies to sensor nodes the security level when data will be published (values: Authentication, Authentication-Encryption, Null).
- KeyTypePub(1flag): Key type publication specifies to sensor nodes the key type when data will be published (GroupKey for the first publication, PairWiseKey for the next publications).
- KeyTypeDistPub(1flag):: Key type is distributed while publication (value: NewPairWiseKey for the first publication).
- Key (8 bytes): key to be distributed (value: GroupKey generated randomly and distributed initially by sink and regenerated in each gradient which rebroadcasts interest message).
- MAC (4 bytes): Message Authentication Code used to check the interest message integrity and that it was broadcast by an authenticated node.

For next secure subscription, Group Key will be used in the place of GlobalKey.

All fields which represented with a flags require together one byte. So the size of the secure interest message is 51 bytes in which 36 bytes are allocated for the original interest message [11].

Table 1 shows pseudo code of the secure subscription started by sink.

TABLE I. SECURE SUBSCRIPTION

Process in sink node	
OPP	Attribut-value Initialized, asdress, TTL,length

SecOPP	level security initialized for subscription and publication;
	if it is the first subscription then
	Key ← GlobalKey;
	Enc_{Key}(Gen(GroupKey)) to store in data gradient cache;
	else
	Key ← GroupKey;
	end if
	MAC_K calculated;

OPP	Broadcast secure Interest Message (IM) ;

When a node receives interest message, it proceeds with pseudo code described in Table2.

TABLE II. INTEREST MESSAGE RECEIVED

Process in Sensor node	

SecOPP	if SecModSub contains Authentication
	if current IM is authenticated then
	if SecModSub contains encryption then
	IM decrypted;
	end if;
	GroupKey of Interest Gradient is decrypted and stored;
	if KeyTypeDistSub contains NewGroupKey
	Enc_{Key}(Gen(GroupKey)) to store in data gradient cache;
	end if
	if SecModSub contains encryption then
	IM encrypted;
	end if;
	MAC_{key} calculated;
	else
	received IM is rejected; quit;
	end if
	end if

	current IM is cached; Address, TTL are assigned;
SecOPP	if SecModSub contains Authentication MAC_{Key} calculated end if;
OPP	Rebroadcast IM;

B. Secure data message routing and Pairwise key sharing

For a sensor node u, when sensed data matches cached interests then a secure data is created. For the first publication, data gradient generates randomly a Pairewise key to share with the best (fastest) interest gradient (ig).

The new format of the sent secure data message will be like this:

$u \rightarrow ig : DM \,||\, Nonce \,||\, SecModPub \,||\, KeyTypePub \,||\, KeyTypeDistPub \,||\, E_{GroupKey}(Key) \,||\, MAC_{GroupKey}$

for next secure publications the pairewise key will be used in the place of globalkey. The size of original data message(DM) [11] is 36. So the size of the secure data is also message 51 bytes.

Table 3 represents the pseudo code of a secure publication.

TABLE III. SECURE PUBLICATION

Process in data gradient sensor node	
SecOPP	if sensed data matches interest entry of the interest cache Data Message is created for the best(fastest) interest gradient; Initialize asdress, TTL,length Attribut-value initialized with sensed data values; Call Secure ForwardData Procedure; end if

Secure forward data procedure is executed both after creations of data message or on receiving a data message. On receiving the first data message the interest gradient decrypts the Pairwise key. Starting from the second sending of data message the sensor node uses the Pairwise key to perform security process. Pseudo-code is detailed in table4.

TABLE IV. SECURE FORWARDDATA

Process in data gradient/interest gradient sensor node	
SecOPP	Level security initialized for data publication if SecModPub contains Authentication if KeyTypeDistPub contains NewPairWiseKey EncGroupKey(Gen(PairWiseKey)); MACGroupKey calculated; else MACPairWiseKey calculated; end if
OPP	Tx DataMessage to the best interest gradient

When an interest gradient (router) receives a data message it proceeds with pseudo-code as follows in table 5.

TABLE V. DATA MESSAGE RECEIVED

Process in interest gradient	

SecOPP	if SecModSub contains Authentication
	if current DataMessage(DM) is authenticated then
	if KeyTypeDistSub contains NewPairWiseKey then
	$Dec_{GroupKey}$(PairWiseKey);
	if SecModPub contains encryption then DM decrypted;
	else received DM is rejected; quit;
	end if

OPP	if received data matches interest entry in interest cache if current interest gradient is sink node data indicated to application level else call ForwardData procedure end if

C. *Rekeying mecanism*

When step *B* is completed the network is already organized in a hierarchical way. Thus, each sensor node shares with its interest gradient a Group key and a Pairwise key. Furthermore, if a sensor is an interest gradient, it shares a Group key with all its members and a Pairwise key with each. The fact which the initial global key can be removed from all sensors nodes.

Moreover, if sensor node leaves the WSN or a compromised node is detected, a non compromised gradient proceed to delete keys which were shared with it. Behind, it can initiate an intrinsic Group key redistribution with a locally secure message. Further more, if a decision to add some sensor nodes to the WSN is token, novel nodes will be pre-loaded with a new Global key. Thereafter, sink node can bootstrap a secure Global key redistribution. This proves that SecOPP can easily maintain backward and forward Secrecy.

V. SECURITY ANALYSIS

In this section we are analyzing the immunity of SecOPP protocol against the most known routing attacks in WSNs[5].

- Replay attacks: if an attacker tries to replay an old interest message, this does not hold because every node stores the last nonce which is a sequential number
- Flooding attack: If the attacker falsifies an interest message the last will not be authenticated and thereafter will be eliminated from sensor node.
- Black hole: if an attacker with high communication capabilities rebroadcasts an interest message it cannot create a black hole in the WSN, because it can't be authenticated by sensor nodes.
- Data flow blocking: in OPP sink node initiates communication by broadcasting interest message which makes it difficult for an adversary to prevent the arrival of the interest message to sensor nodes.
- Physical attacks: In hostile environment, some sensor nodes can be captured and tampered. Obviously, the most sensitive information is shared keys. The impact of such attack affects only secure links with immediate neighbors and not the whole network.
- Brute force attack: SecOPP protocol permits to redistribute Group keys and Pairwise keys for new subscription which limits the effect of this attack.

VI. SIMULATIONS AND RESULTS

SecOPP protocol is implemented for TinyOS using NesC language and simulated under TOSSIM [13]. It is viable for implementation in resource-constrained platforms like Telos motes or MicaZ. Table 6 recapitulates the size of messages exchanged in OPP and SecOPP. The 15 added bytes permit to store the security level used for current message, the message authentication code(Mac) and the shared key.

TABLE VI. SIZE OF EXCHANGED MESSAGES

Messages	Protocol	Size
Original interest message	OPP	36 bytes
Secure interest message	SecOPP	51 bytes
Original data message	OPP	36 bytes
Secure data message	SecOPP	51 bytes

We simulate a subscription to temperature in the deployed field. Various measures are taken for the three security levels: security disabled (level 0), authentication-key sharing (level 1), authentication-confidentiality-key sharing(level 2) .

Interests to temperature are broadcast in the WSN with such parameters:

- Attribute/value: temperature > 40°C,
- Interest expiration period = 1500 s,
- Sending frequency = 3,
- Interval = 30 s.

The obtained results show the scalability of the proposed secure protocol. Indeed, sensed data from all sensor nodes can reach securely the sink node for different network size.

Figure 3 shows necessary time to gathering information from WSNs of different sizes. It is clear that time to gather information is more important where size of WSN increases. This is caused by the rise of hops number on the routing paths.

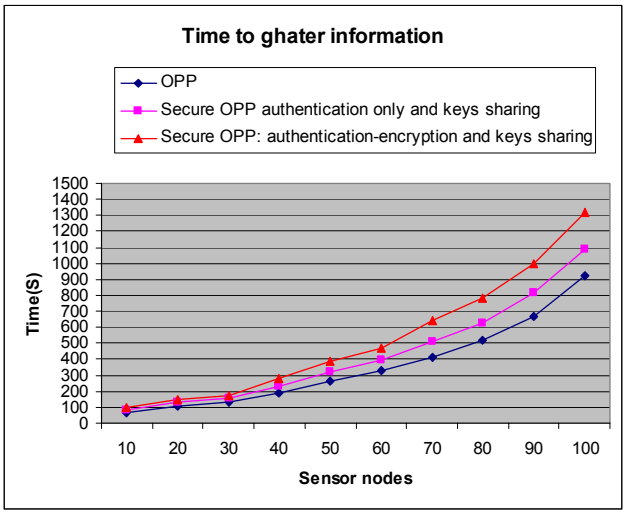

Figure 3. Time to gather information

Energy consumption is simulated with PowerTOSSIM which uses mica2 energy model. Figure 4 represents an average of energy consumption of SecOPP for different network size. Indeed, the shape of curves is far from being exponential, which shows the effectiveness of SecOPP. Moreover the increase in energy consumption for security level 1 and level 2 are respectively about 15% and 21% more than level 0 where security is disabled. We conclude that SecOPP protocol provides low energy consumption for WSNs.

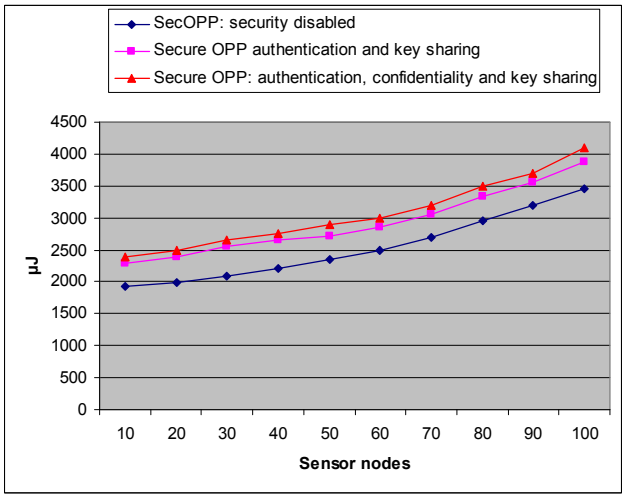

Figure 4. Average of consumed energy

VII. CONCLUSION

Our protocol SecOPP gives an efficient secure solution to the data centric routing protocol OPP diffusion. It provides security services, keying and rekeying mechanism to establish and refresh Group and Pairwise key. All of this is obtained without using a key distribution center. Security analysis shows that proposed secure protocol can withstand several possible routing attacks in the network. Additional computations and communications are not significant. In fact, Simulation results shows that SecOPP is energy efficiency and scalable. In consequence, SecOPP protocol satisfies the main security goals fixed in advance.

REFERENCES

[1] Sencun Zhu, Sanjeev Setia and Sushil Jajodia, " LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", ACM Transactions on Sensor Networks, November 2006.

[2] Yang Xiao and all, 'A survey of key management schemes in wireless sensor networks', science direct computer communication 2007.

[3] Seyit A. Camtepe and Bulent Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", Technical Report TR-05-07-Rensselaer Polytechnic Institute 2005.

[4] Junqi Zhang, Vijay Varadharajan ,"Wireless sensor network key management survey and taxonomy", Science Direct, Journal of Network and Computer Applications. Elsevier 2009.

[5] C. Karlof and D. Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures," Elsevier's Ad-Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, 2003.

[6] An Liu and Peng Ning, "TinyECC: A Configurable Library forElliptic Curve Cryptography in Wireless Sensor Networks", in proceedings of 7th international conference on Information processing in sensor networks, 2008.

[7] C. Karlof, N. Sastry, D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 03 – 05 November 2004, New York, NY, USA: ACM Press, 162 – 175. 2004.

[8] L. Eschenauer, V.D. Gligor, "A key management scheme for distributed sensor networks", in: Proceedings of the 9th ACM Conference on Computer and Communication Security.

[9] Kemal Akkaya, Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County Baltimore, MD 21250.

[10] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin , John Heidemann, Fabio, Silva, "Directed diffusion for wireless sensor networking", IEEE/ACM Transactions on Networking, Volume 11 Issue 1, February 2003.

[11] Manamohan Mysore and all, "TinyDiffusion in the Extensible Sensing System at the James Reserve", http://www.cens.ucla.edu/~mmysore/ Design/OPP/.

[12] Min-Sook Jin, Hosung Park, Euisin Lee, Soochang Park and Sang-Ha Kim, "A Data Dissemination Model Base on Content-based Publish/Subscribe Paradigm in Large-scale Wireless Sensor Networks", in IEEE WCNC 2009.

[13] Philip Levis, Nelson Lee, Matt Welsh, David Culler, "TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications", SenSys, 2003.