A study of Intrusion-tolerant routing in Wireless Sensor Networks

V. H. La <vinh_hoa.la@telecom-sudparis.eu>
A. R. Cavalli <ana.cavalli@telecom-sudparis.eu>
Telecom SudParis
9 rue Charles Fourier, 91011 Evry, France

Abstract. Wireless Sensor Networks (WSNs) emerge recently as one of the most attractive research subjects. The resource- constraint characteristics of WSNs limit the secure design and development of security protocols for them. Whilst, sensor nodes those usually operate in unattended and even harsh environments, are prone to failures and are vulnerable to malicious attacks. For reliable and secure communications in WSNs, intrusion-tolerant routing becomes a critical attribute that should be integrated into WSNs. In this paper, we study two intrusion- tolerant routing protocols for WSNs, namely INSENS and ITSRP, as well as analyze the intrusion-tolerant properties gained from these two propositions. Simulation and performance analysis have proved that both of them are practical.

Keywords: intrusion-tolerance; wireless sensor networks; routing; attack-tolerance

1. Introduction

In the current era, WSNs are rapidly emerging as an important area in both the research community and the public, due to the unique features (limited energy lifetime, slow embedded processors, severely constrained memory and low-bandwidth radios). For example, Waspmote [1], the modern open source sensor device distributed by Libelium, contains simply a 14 MHz micro-processor, 3.3 V-4.2 V battery voltage, 8 KB SRAM, 128 KB flash memory and 4 KB EEPROM to save sensed data, run and operating system and application programs. These resource constraints limit the degree of encryption, decryption, and authentication, in addition to physical security risks of being deployed in inaccessible terrains or unattended and even hostile environment, thus, the concept security and WSNs were likely contradictory. The integration of an intrusion detection system seems to be too expensive in terms of resource. WSNs are exposed to a variety of security threats in addition to the ones normally observed in traditional wired and wireless networks. Therefore, it is essential to take intrusion tolerant concept into consideration to sustain the sensor network functionalities without interruption despite malicious attacks and sensor node failures.

Our paper aims to present an analysis on two existing intrusion-tolerant routing protocols proposed for WSNs, namely INSENS and ITSRP. They are, in our opinion, two best intrusion-tolerant routing protocols so far. We attempt to briefly describe them and mainly focused our analysis on intrusion-tolerance properties. Simulations and performance analysis will be also discussed.

The rest of this paper is organized as follows: Section 2 is devoted to describe and assess INSENS and ITSRP. Section 3 contains the simulation results and performance analysis. Finally, we summarize our study as well as propose the future work in Section 4.

2. Intrusion-tolerant Routing Protocols in WSNs

Intrusion tolerance [5], [6], [7] is generally understood as the capability to continue to function properly with minimal degradation of performance, despite intrusions or malicious attacks. A great deal of work has been done to address the sensor network security problems recently so that the WSNs can tolerate and/or prevent intrusions [3], [4]. In the following subsections, we attempt to identify two current approaches used for achieving intrusion-tolerant routing- one of the most critical features in WSNs.

2.1 INSENS- INtrusion-tolerant routing protocol for wireless SEnsor NetworkS

INSENS [15], [16], [17] could be subdivided into 2 phases: ***Route Discovery*** phase and ***Data Forwarding*** phase. The goal of the first phase is to collect topology knowledge and to construct appropriate forwarding tables at every node. Whilst, the second phase simply enables forwarding of data from each sensor node to the base station and vice versa. It is worth mentioning that every communication between nodes is one-way forwarded (unicast) via base station. The Route Discovery phase is composed of three rounds: ***Route Request, Route Feedback, and Computing and Propagating Multi-path Routing Tables.***

In the beginning (or when the topology may have changed substantially because of nodes' mobility), the base station floods (limited flooding) a *request message* to all the reachable sensor nodes in the network. After receiving a *request message* for the first time, a sensor node *x* broadcasts in turn another *request message* that includes a *path* from the base station to *x* and also the *identity* of *x*. Whenever receiving duplicate request messages, it records the *identity* of the sender as a neighbor, but stop re-broadcasting the duplicate request. The base station authenticates the *feedback messages* received from sensor nodes (authentication manner will be further discussed in the follow parts of this paper). After that, it constructs a topological picture of the network from the authenticated neighborhood information, computes the forwarding tables for each sensor node, and sends the

tables respectively to nodes using a *routing update message*. To address the influences of compromised nodes, INSENS builds redundant multi-path routing tables containing disjoint paths. Therefore, even if a single node or path is taken down by an intruder, secondary paths will substitute.

The main idea of this approach is to add *OWS* (one-way sequences) field and the *MAC* (Message Authentication Code) field *(MACR* and *MACF)*, that support the intrusion-tolerant properties of INSENS, into message format. First of all, the base station uses one-way sequences (OWS) proposed by *μTESLA* protocol [8] F to generate a sequence of numbers K0, K1... Kn, such that Ki = F(Ki+1), where 0 < i < n and F satisfies the condition that it is computationally infeasible to compute Ki+1 in a limited time by only knowing F and Ki. Initially, every node is pre-configured to know K0 and F. In the first Route Discovery phase, the base station includes K1 in the request message that it broadcasts. Similarly in general, the base station uses Ki in the ith Route Discovery phase. After receiving a request message, a node verifies if the sequence number did indeed originate from the base station by checking whether K0 = Fi (Ki). A malicious node would be computationally impossible to guess the next OWS. As a result, a compromised node cannot spoof the base station by generating new OWS. On the other hand, a sensor node will save the most up-to-date or freshest OWSfresh that it has just seen from the base station. This fact resists an intruder to disrupt the network by using old OWS to flooding old request messages.

In fact, a malicious node is still possible to flood a modified request message in using the current OWS from a valid request message that it has just received from the base station. Such an attack is discussed as ***rushing attack*** in [2]. However, nodes in the tree (Fig. 1), that are closer to the base station than the malicious node m, will receive the valid request message first. These nodes will drop the intruder's spurious request messages received later because, as mentioned above, nodes do not rebroadcast duplicate request messages (contain the same OWS). Even when neighboring nodes of m accept to forward the fake request message created by m, they forward only once. DOS attack, thus, is no longer in our concerns. Nevertheless, an unsolved issue in primary INSENS is that attacker could pack a fake path into its spurious request message or drop the request message instead of forwarding it. Some nodes can be harmed (not getting a request message or not being able to forward their feedback message to the base station in the second round) but, as shown in Fig. 1, the damage is locally confined to the nodes nearest to and downstream from the intruder. This conclusion seems to be logical but remains intuitive and needs further evaluation to know whether such damage can still seriously disrupt the network.

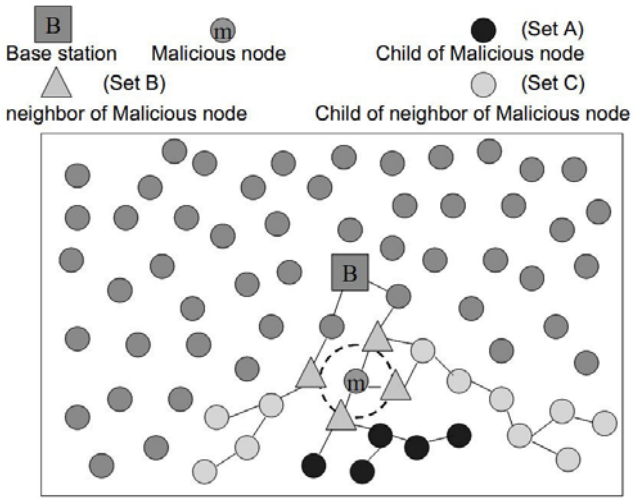

Fig. 1. The damage inflicted by a malicious node m is confined to a localized portion of the sensor network, i.e., nodes downstream from m and downstream from neighbors of m

In addition to OWS, keyed MAC (Message Authentication Code) algorithm is another factor that provides intrusion- tolerant properties for INSENS. Each sensor node is initially configured with a separate *secret key* that is shared only with the base station. When a node *x* receives a request message for the first time, before forwarding it, *x* appends its identity to the path list, and then generates a MAC of the complete new path with its key: $MACR_x = MAC\ (size|path|OWS|type,\ key_x)$ where "|" denotes concatenation. The value of MACR is also appended to the request message that is then forwarded downstream. This MACR field will eventually be exploited by the base station to verify the integrity of the path contained in the packet. Additionally, even if a node is compromised, only its secret key will be revealed, so an intruder cannot compromise the entire network.

In the second round (*Route* Discovery-*Route Feedback*), keyed MAC is applied one more time to protect the integrity of feedback messages. List of neighbors *nbr_info* and the path *path_info* to a node x are protected by the following keyed $MACF_x$: $MACF_x = MAC\ (path\ info\ |\ nbr\ info\ |\ OWS\ |\ type,\ key_x)$.

In feedback messages, *parent info* field determines a child's upstream neighbors and takes part in forwarding the feedback message to the base station. Using only identity I_p would be an obvious vulnerability because it does not require the casual intruder to have either any knowledge of the local topology or of the current state of the topology discovery process. To address this concern, INSENS requires a child node to put its parent's $MACR_p$ that is included in the parent's original request message into the *parent_info* field. This $MACR_p$ is tightly linked with the current state of the OWS request-feedback cycle, as well as to the path to the child node. In

other words, the $MACR_p$ plays a role as not only an addressing function but also a security function. A casual attacker, that only knows *node id*, would be unable to forward a spurious feedback message.

2.2. ITSRP- Intrusion Tolerant Secure Routing Protocol

ITSRP [19] is a novel secure routing protocol which focuses on the design of some fields to emphasize the security accounting to the key exchange, but not result in the complexity of the protocol. The main target of the ITSRP is to tolerate damage caused by an intruder who has compromised deployed sensor nodes and is intent on injecting, modifying, or blocking packets [20], but in a reasonable price regarding energy factor. As any other routing protocol, ITSRP consists of following steps: *path discovery* (sink node informs to other nodes that it is in need of network topology), *path reverse* (nodes send back topology information to help sink node build up routing tables) and *data transfer* (simply based on routing tables).

The general idea to achieve intrusion-tolerance in ITSRP is derived from the procedure to establish a secret session key *SK* whenever a source node N_0 wants to send a confidential message *M* to the sink node N_n but it lacks neither an available *route path* nor a *shared session key* with N_n. It is worth mentioning that each node is initially issued a Distributed Key (*DK*) that is shared only between itself and the sink node (e.g., the base station) and that each node store a *local route table* (LRT) containing entries whose format is demonstrated as follow:

Table 1. Format of an entry in LRT

Tag	Ancestor	Successor	Energy	Lifetime

In the first phase, N_0 must establish a *route path* and a *session key SK* uniquely shared with N_n through intermediate nodes. The source node N_0 first generates the unique *Tag* for this route and realizes these following steps:

(1) - Select randomly a secret session key SK_0, compute the energy consumption E_0 for transmitting the message M.

(2) - Set $M_0 = [Tag|N_0|N_n|SK_0]$ ("|" depicts the concatenation) and encrypt M0 in using the DK0: C0 = Edk (M0).

(3) - Encapsulate the packet [Tag|Nn|C0|E0] and broadcast it to all nodes within its wireless transmission range.

(4) - Store the entry (Tag, 0, ?, E0, T0) to its LRT0 where T0 is the timer for the route and starts when the entry is added. Each node close to N_0 node receives packet $[Tag|Nn|C_0|E_0]$, it checks and drops if this packet has been already received before. Otherwise, it broadcasts this packet within its range and store $(Tag|N_0|?|E_0|T_0)$ in its LRT_1. Without loss of generality, assuming that packet passes the intermediate nodes N_1, N_2... N_{n-1} and reaches the sink N_n. Node N_i stores $(Tag|N_{i-1}|?|E_0|T_i)$ in its LRT_i.

In the second phase, the sink node N_n must send back to the source node N_0 the reverse path. N_n works as follows:

(1) - Knowing DK_0, the sink node N_n is able to decrypt C_0 to get M_0, and then get SK_0.

(2) - Make $M_n = [Tag|N_0|N_n|SK_0]$ and use DK_0 to encrypt M_n as C_n.

(3) - Look up its ancestor node N_{n-1} according to *Tag* in its LRT_n, then use DK_{n-1} to encrypt *Tag* as C_{n-1} and send $[C_n|C_{n-1}]$ to N_{n-1}.

When the node N_{n-1} receives $[C_n|C_{n-1}]$ from N_n, it works as follows:
(1) - Use DK_{n-1} to recover *Tag*.

(2) - Look up in its LRT_{n-1} according this *Tag* and update the entry saved from the first phase: $(Tag|N_{n-2}|N_n|E_0|T_{n-1})$.

Similarly to the end, N_0 gains the entry $(Tag, 0, N_1, E_0, T_0)$ in its LRT_0. Not only has the route from N_0 to N_n been discovered but also a shared session key *SK* between of them has been established.

Indeed, ITSRP is intrusion tolerant firstly because of the redundancy in possible paths. For a route, there are multiple paths possibly used to reduce the failure rate caused by intruder. Furthermore, ITSRP provides significant protection against a variety of malicious attacks during the routing set up phase as well as during the data forwarding phase, especially in comparison with the naive Directed Diffusion routing protocol.

In fact, different salient attacks in WSNs routing have been described in literature [2], including Sinkhole attacks, Wormhole attacks and Sybil attacks that induce incorrect routing information to provoke incorrectly forwarding messages. In a sinkhole attack, a malicious node presents itself having the shortest path to a well-known destination, e.g., a sink node. In networks that apply a routing scheme allowing nodes to select their routing path based on neighborhood routing information, a sinkhole attack can lead to incorrect routing paths towards the malicious node. The malicious node, thus, can disturb the routing activities as well as collect illegitimately data from networks. However, the distributed key management and the mechanism to build a route path of ITSRP protect itself from sinkhole attacks. A malicious node has no possibility to pretend a sink node, as well as pretend to belong to the shortest path without knowing the distributed key. In a Sybil attack, a malicious node forges multiple fake identities and then deceives other sensor nodes using those fake identities. This attack is eliminated from ITSRP because of the distributed key management. Each node is not only identified by its ID but also by its DK that is shared secretly between itself and sink node. The forgery of sink node is also not feasible without knowledge about DKs. Rushing attacks (that was formerly discussed above in INSENS's section) are also avoided

out of our concerns because each message forwarded by a node is encrypted with a distributed key (in path discovery phase and path reserve phase) or with a session key (in data transfer phase). For HELLO flood attacks where an adversary with a powerful transmitter reaches every node in the network, and pretends to be a neighbor, ITSRP assure each pair of neighboring nodes to establish a secure communication channel by agreeing on a unique secret key DK between two neighboring nodes, which is bidirectional. Each legitimate node keeps only an ancestor and a successor in the routing map (LRT), so each node only accepts and forwards one copy of the same packet, otherwise, drop them. This fact defenses against any attacker contriving HELLO flood attack.

In [19], the authors affirm that their proposition is immune to Wormhole attacks in which two malicious nodes exchange their routing information using a fast and secure channel or tunnel, and then trap or warp the routing paths of their neighbor nodes. However, in our opinion, a wormhole attack can still harm ITSRP, even though the probability of this event can be very low. In fact, in the path discovery phase, each node after receiving a path discovery packet will broadcast it within its wireless communication range. This packet can be logically duplicated but will be actually drop very fast because one node will allow to receive this packet only one time and drop whenever detect the duplication. The shortest path will be found quickly due to the quick rate of wireless communication (in fact that depends on which mean of wireless communication used in the network, e.g., Wifi, GPRS, Bluetooth, ZigBee, etc.). If somehow two malicious nodes can exchange this packet faster than legitimate nodes, they are still able to set up a tunnel and thus, generate an incorrect route path. After that, they can disrupt this tunnel or do whatever they want because they have gained a very powerful role in routing activities.

3. Analysis and performance evaluation

Firstly, by theoretically analyzing aforementioned protocols, we affirmed that they, indeed, are able to tolerate some critical attacks and kinds of intrusion. However, they have themselves shortcomings that should be accomplished by further researches. Table 2 summaries our analysis.

Table 2. Intrusion-tolerant properties and shortcomings of INSENS and ITSRP

Routing protocol	Intrusion/Attack tolerance	Attack “intolerance”
INSENS	Redundancy Battery drain attack Memory exhaustion attack DOS/ DDOS attack Rushing attack	Rushing attacks are not completely solved. Although the influences are restricted in a local partition of the network but further theoretical and practical evaluations deserve more research and consideration
ITSRP	Redundancy (multiple paths) Sink hole attack Sybil attack HELLO flood attack Rushing attack	Wormhole attacks are still able to occur despite the low probability

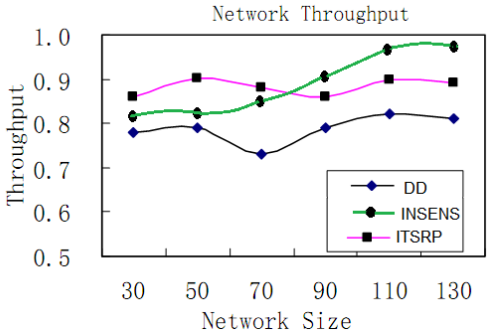

Fig. 2. Average network throughput of ITSRP and Directed Diffusion

Secondly, to evaluate the performance of INSENS and ITSRP, we performed a simulation by **OMNeT++** integrated Castalia plug-in. We simulated a rectangular region of area 150m x 150m in which the wireless sensor nodes were deployed and 25 percent of nodes misbehave. In Fig. 2, we witness that throughput of three metrics decreases more or less because of nodes misbehave. However, the network experiences a considerable decrease in DD (Directed Diffusion) protocol, but only a slight change in INSENS or ITSRP. This result proves one more time the intrusion-tolerance properties of ITSRP and declares that INSENS is better than ITSRP if the number of sensor nodes enormously increases.

4. Conclusion and perspectives

In this paper, we have presented an analysis on INSENS and ITSRP that are, from our point of view, two best intrusion- tolerant routing protocols insofar. We have briefly described these two protocols and mainly focused our analysis on intrusion-tolerance properties. The Table 2 summarizes the main intrusion-tolerant properties assured by INSENS and ITSRP as well as missing issues that could not be thoroughly solved. We have also analyzed the performance to evaluate the practicality of both two protocols. We believe that our paper is useful for WSNs researchers as a study on the state of the art and for developers in implementing a secure WSN. In future, we would like to implement further experiments to

compare the performance of INSENS with ITSRP as well as simulate some attack scripts to verify the resilience and stability. The missing issues mentioned in Table 2 are also future works that we would like to accomplish.

References

[1]. Libelium Comunicaciones Distribuidas S.L. “Waspmote Datasheet”, 2014

[2]. Akyildiz I, SuW, et al. “Wireless sensor networks: a survey”, in Computer Networks, pp. 393-422, 2002.

[3]. Ruiping Ma, Liudong Xing, Howard E. Michel. “Fault-Intrusion Tolerant Techniques in Wireless Sensor Networks”, in 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 85- 94, 2006.

[4]. Liang-min Wang, Jian-feng Ma, Chao Wang, A.C. Kot. “Fault and intrusion tolerance of wireless sensor networks”, in 20th International Parallel and Distributed Processing Symposium, 2006.

[5]. Yves Deswarte, David Powell, “Intrusion-tolerance on the Internet (Tolrance aux intrusions sur Internet)”, in Presentation slide, LAAS- CNRS, Toulouse, France, 2005.

[6]. B.B. Madan and K.S. Trivedi, “Security modeling and quantification of intrusion tolerant systems”, in ISSRE, 2002.

[7]. Feiyi Wang, Raghavendra Uppalli, Charles Killian, “Analysis of tech- niques for building intrusion tolerant server systems”, in Military Communications Conference MILCOM ’03 IEEE, pp. 729 - 734 Vol.2, 2003.

[8]. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”, in Journal of Wireless Networks, Volume 8, Issue 5, pp. 521- 534, Sept. 2002.

[9]. Chris karlof, Naveen Sastry, David Wagner. “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks”, in Proceedings of the 2nd international conference on Embedded networked sensor networks, pp. 162-175, 2004.

[10]. Soumya Basu, M.Pushpalatha. “Analysis of energy efficient ECC and TinySec based security schemes in Wireless Sensor Networks”, in IEEE International Conference on Advanced Networks and Telecommunication Systems (ANTS), pp. 1 - 6, 2013.

[11]. Ajay Mahimkar, Theodore S. Rappaport. “SecureDAV: a secure data aggregation and verification protocol for sensor networks”, in IEEE Global Telecommunications Conference (GLOBECOM), pp. 2175 – 2179, Vol.4, 2004.

[12]. Leonardo B. Oliveira, Hao Chi Wong, Antonio A. Loureiro. “LHA- SP: secure protocols for hierarchical wireless sensor networks”, in 9th IFIP/IEEE International Symposium on Integrated Network Manage- ment, pp. 31 - 44, 2005.

[13]. D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar. “Next century challenges: Scalable coordination in sensor networks ”, in Mobile Computing and Networking , pp. 263 – 270, 1999.

[14]. Maha Sliti, Mohamed Hamdi, Noureddine Boudriga. “Intrusion-tolerant framework for heterogeneous Wireless Sensor Networks”, in The 7th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009, pp. 633- 636, May 10-13, 2009.

[15]. J. Deng, R. Han, and S. Mishra. “INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks”, Poster paper in 23rd IEEE International Conference on Distributed Computing Systems, 2003

[16]. J. Deng, R. Han, and S. Mishra. “INSENS: Secure and Intrusion Tolerant Routing for Wireless Sensor Networks”, Technical Report CU-CS 939-02. Department of Computer Science. University of Colorado, Boulder, CO. November 2002.

[17]. J. Deng, R. Han, and S. Mishra. “A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks”, in 2nd IEEE International Workshop on Information Processing in Sensor Networks, 2003

[18]. Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, Ahmed Helmy. “Secure Locations: Routing on Trust and Isolating Compromised Sensors in Location-Aware Sensor Networks”, in SenSys’08, Los Angeles, California, USA, ACM 1-58813-707-9/03/0011, 2008

[19]. Jiliang Zhou, Caixia Li , Qiying Cao and Yu Shen, “An intrusion-tolerant secure routing protocol with key exchange for wireless sensor network”, in International Conference on Information and Automation-ICIA 2008, pp. 1547 - 1552, 2008.

[20]. L.M. Feeney. “An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks”, in Mobile Networks and Applications, pp. 239 - 249, 2001.

Исследование отказоустойчивой маршрутизации в беспроводных сенсорных сетях

В. Х. Ла <vinh_hoa.la@telecom-sudparis.eu>
А. Кавалли <ana.cavalli@telecom-sudparis.eu>
Telecom SudParis, 9 rue Charles Fourier, 91011 Evry, France

Аннотация. Развитие технологий и снижение стоимости беспроводных сенсорных систем привело к открытию новых областей для их применения и повышению требований к обеспечению безопасности и надежности сетей. Ограничения ресурсов узлов беспроводных сенсорных сетей приводят к жестким рамкам для реализации безопасных протоколов их взаимодействия. Так как сенсорные узлы работают, как правило, в неконтролируемой или даже враждебной среде, они подвержены отказам и уязвимы для атак. Для обеспечения надежности и безопасности взаимодействия сенсоров в сети отказоустойчивая маршрутизация становится ключевым элементом, который должен быть реализован в беспроводных сенсорных сетях. В данной работе исследуются два отказоустойчивых протокола маршрутизации, INSENS и ITSRP, для которых проводится анализ параметров их устойчивости к атакам. Моделирование и анализ быстродействия показали, что оба протокола достаточно хороши с практической точки зрения.

Ключевые слова: отказоустойчивость; беспроводные сенсорные сети; маршрутизация; устойчивость к атакам.

Список литературы

[1]. Libelium Comunicaciones Distribuidas S.L. “Waspmote Datasheet”, 2014
[2]. Akyildiz I, SuW, et al. “Wireless sensor networks: a survey”, in *Computer Networks*, pp. 393-422, 2002.
[3]. Ruiping Ma, Liudong Xing, Howard E. Michel. “Fault-Intrusion Tolerant Techniques in Wireless Sensor Networks”, in *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, pp. 85- 94, 2006.
[4]. Liang-min Wang, Jian-feng Ma, Chao Wang, A.C. Kot. “Fault and intrusion tolerance of wireless sensor networks”, in *20th International Parallel and Distributed Processing Symposium*, 2006.
[5]. Yves Deswarte, David Powell, “Intrusion-tolerance on the Internet (Tolrance aux intrusions sur Internet)”, in *Presentation slide*, LAAS- CNRS, Toulouse, France, 2005.

[6]. B.B. Madan and K.S. Trivedi, “Security modeling and quantification of intrusion tolerant systems”, in *ISSRE*, 2002.
[7]. Feiyi Wang, Raghavendra Uppalli, Charles Killian, “Analysis of techniques for building intrusion tolerant server systems”, in *Military Communications Conference MILCOM ’03 IEEE*, pp. 729 - 734 Vol.2, 2003.
[8]. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”, in *Journal of Wireless Networks*, Volume 8, Issue 5, pp. 521- 534, Sept. 2002.
[9]. Chris karlof, Naveen Sastry, David Wagner. “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks”, in *Proceedings of the 2nd international conference on Embedded networked sensor networks*, pp. 162-175, 2004.
[10]. Soumya Basu, M.Pushpalatha. “Analysis of energy efficient ECC and TinySec based security schemes in Wireless Sensor Networks”, in *IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)*,pp. 1 - 6, 2013.
[11]. Ajay Mahimkar, Theodore S. Rappaport. “SecureDAV: a secure data aggregation and verification protocol for sensor networks”, in *IEEE Global Telecommunications Conference (GLOBECOM)*,pp. 2175 - 2179 Vol.4, 2004.
[12]. Leonardo B. Oliveira, Hao Chi Wong, Antonio A. Loureiro. “LHA- SP: secure protocols for hierarchical wireless sensor networks”, in *9th IFIP/IEEE International Symposium on Integrated Network Management*, pp. 31 - 44, 2005.
[13]. D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar. “Next century challenges: Scalable coordination in sensor networks, in *Mobile Computing and Networking* , pp. 263270, 1999.
[14]. Maha Sliti, Mohamed Hamdi, Noureddine Boudriga. “Intrusion-tolerant framework for heterogeneous Wireless Sensor Networks”, in *The 7th IEEE/ACS International Conference on Computer Systems and Applications*, AICCSA 2009, pp. 633- 636, May 10-13, 2009.
[15]. J. Deng, R. Han, and S. Mishra. “INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks”, Poster paper in *23rd IEEE International Conference on Distributed Computing Systems*, 2003
[16]. J. Deng, R. Han, and S. Mishra. “INSENS: Secure and Intrusion Tolerant Routing for Wireless Sensor Networks”, Technical Report CU-CS 939-02. Department of Computer Science. University of Colorado, Boulder, CO. November 2002.
[17]. J. Deng, R. Han, and S. Mishra. “A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks”, in *2nd IEEE International Workshop on Information Processing in Sensor Networks*, 2003
[18]. Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, Ahmed Helmy. “Secure Locations: Routing on Trust and Isolating Compromised Sensors in Location-Aware Sensor Networks”, in *SenSys’08, Los Angeles, California, USA, ACM 1-58813-707-9/03/0011.*, 2008
[19]. Jiliang Zhou, Caixia Li , Qiying Cao and Yu Shen, “An intrusion-tolerant secure routing protocol with key exchange for wireless sensor network”, in International Conference on Information and Automation-ICIA 2008, pp. 1547 - 1552, 2008.
[20]. L.M. Feeney. “An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks”, in Mobile Networks and Applications, pp. 239 - 249, 2001.