Event-based Trust Framework Model in Wireless Sensor Networks

Haiguang Chen[1,2], Huafeng Wu [2,3] , Jinchu Hu[1], Chuanshan Gao[2]
[1]*Mathematic and Science College* *Shanghai Normal University* *Shanghai, P. R. China, 200234* *{chhg, hujc}@shnu.edu.cn*
[2]*Dept. of Comp. Sci. & Engr.* *Fudan University* *Shanghai, P. R. China, 200433* *{hgchen, wuhuafeng, cgao}@fudan.edu.cn*
[3]*Merchant Marine College* *Shanghai Maritime University* *Shanghai, P. R. China, 200135*

Abstract

The security of wireless sensor networks is ever more important nowadays. Most of the proposed security protocols in wireless sensor networks are based on authentication and encryption. But all of them only address part of the problem of security in wireless sensor networks. Recently, the use of reputation and trust systems has become an important secure mechanism in wireless sensor networks. In this paper we propose a new protocol ETSN to construct a trust framework model in wireless sensor networks. The ETSN will be more suitable than ATSN and RFSN in wireless sensor networks. The simulation results and analysis show that our scheme not only can fast detect the malicious nodes and scale well for wireless sensor networks, but also can distinguish trust rating with different event.

1. Introduction

Wireless sensor networks (WSNs) have wide applications due to these sensor nodes ease of deployment, such as environment monitoring, rescue missions, and smart houses. A lot of interest and effort are being focused on this new network topic. The sensor networks are constructed by a large number of nodes with ultra-low power computation and communication units [16]. An adversary can control a sensor node undetectably by physically compromising the node and use the captured nodes to inject faulty or false data into the network system disturbing the normal cooperation among nodes. Authentication and cryptographic mechanisms alone cannot be used to full solve this problem because internal adversarial nodes will have valid cryptographic keys to access the other nodes of the networks.

A new kind of mechanism for security in WSNs [2, 3, 5] has been presented, which is trust system. It borrows tools from economics, statistics and mathematics analysis with cryptography. The sensor nodes cannot afford the computation of reputation and trust rating, so we deployed some agent nodes in WSNs to monitor the behaviors of sensor nodes and to compute the reputation and trust rating for these sensor nodes of different events. These nodes only need to receive the trust rating from the agent node and update the trust rating. ATSN was proposed by Chen el al [5], but the scheme cannot distinguish different event.

In this paper, we propose an event-based trust framework model for WSNs. The sensor node has different trust rating for different event. Our model use watchdog scheme to observe the behavior in different events of these nodes and broadcast their trust ratings. The main contributions in our paper are listed as follows:

1. Offer a distributed event-based trust framework model to detect malicious sensor nodes in different event.
2. Develop a new protocol ETSN to deal with the malicious sensor nodes in different event.
3. Propose a new direction in trust system for wireless sensor network.

The rest of the paper is organized as follows. Section 2 briefly describes the related works about security in reputation and trust system for WSNs. Section 3 describes the event-based trust framework model. Section 4 presents trust aging and trust distribution. Section 5, the implementation of event-based trust framework model is described and simulation results are shown. The conclusion is drawn in section 6.

2. Related Works

This section will briefly introduce some security works in WSNs. As we know if we have no adequate security, the applications of WSNs could be curtailed. Several proposals have been existed, but all based on cryptography to ensure secure communication among these resource constrained nodes [6, 7, 8, 9, 10]. And some IDSs have been used for security in WSNs [11, 12]. But both cryptography and IDSs cannot sufficient for the unique characteristics and novel misbehaviors

978-0-7695-3187-8/08 $25.00 © 2008 IEEE
DOI 10.1109/NAS.2008.33

encountered in WSNs. The reputation and trust systems have been proved useful mechanism to address the threat of compromised or faulted entities. They operated by identifying selfish peers and excluding these entities from the network. Trust system has begun to be used in Ad-hoc networks and WSNs.

RFSN[1] is the first reputation and trust-based model designed and developed exclusively for sensor networks, which using watchdog mechanism to build trust rating. But the watchdog cannot record all the behavior due to its own fault, so there is uncertainty in the trust system.

DRBTS [15] is a special case to build a distributed model in location-beacon sensor networks using both first-hand and second-hand information.

CONFIDANT[14] is a routing protocol in MANETs which is a distributed, symmetric reputation model using both first-hand and second-hand information for updating reputation values. However, it easy to be bad-mouth attack if we use second-hand information. And most of the trust system is unsymmetrical.

ATSN [5] is an agent-based trust model for WSNs, but it can't distinguish different events which effect the trust rating, and all the events has the same affects. Each one sensor node has one trust rating value for different events, that scheme is not suitable for WSNs due to its constrained resource. As we known that a sensor node should do best as it can.

P.Resnick et al. [13] is a centralized reputation system. In the system, every entity requests the trust rating of the other's from the central node. The central node is a bottleneck for accessing the trust rating table and they all have a single point of failure and do not scale well, it cannot be used in large scale WSNs.

In this paper, we propose an ETSN protocol to detect the malicious or faulted nodes in different events. The focus of our work is to build a distributed event-based trust framework model in WSNs.

3. Trust Framework Model

In section 2, we have described some related research work on reputation and trust system in WSNs. But our Event-based trust framework model (ETSN) is different from RFSN [1] and ATSN [5], S.Ganeriwal, et al [1] use the watchdog mechanism to collect data samples and build reputation R_{ij} , and then get the trust $T_{ij} = \frac{\alpha_j + 1}{a_j + \beta_j + 2}$. But the watchdog maybe cannot record all the positive outcomes or negative outcomes for a certain event due to the attacker or fault of the node's hardware. So, we just can sure for a certain event, the watchdog get at least α_j positive outcomes and β_j negative outcomes. The above trust T_{ij} ignores uncertainty. In ATSN[5], trust management model has been used the uncertainty factor as Chen, et al [2] presented. But the scheme cannot tell the bad mistake from occasional mistaken. If the sensor does well in every unimportant event such as data collection, packet transmission and correct data conjunction, then it gets a high trust rating. After that, if the WSNs happened doing an urgent or important event, the sensor nodes begin some malicious behavior such as select forward packet. But its neighbor nodes continue cooperating with the malicious node due its trust rating is still high enough. All the forenamed schemes can not deal well with this problem.

In our event-based trust framework, the trust rating is depended on different event of the sensor nodes in WSNs. It means that different event of the sensor node has different trust rating, which also means a sensor node has several trusting rating stored in its neighbor nodes.

And we also consider the scarce resource of sensor nodes. Our scheme similar as [5] that only needs the agent node equipped with watchdog to monitor the different event of other sensor nodes within its radio range. The agent nodes compute and distribute other sensor nodes' trust rating of different event. These sensor nodes receive the trust rating of different event from the agent node and decide if cooperate with other sensor nodes according to their trust rating of a certain event.

3.1 System Architecture

Our event-based trust framework runs at the every agent node which has strong competence to compute, large storage and memory. The agent node uses watchdog scheme to monitor all kind of event happened in sensor nodes within its radio range and functions in a completely distributed manner. Every agent node maintains trust table about a subset of these nodes and unlike RFSN [1], every node has watchdog and need to maintain the trust of other nodes. And in our event-based trust framework, every sensor node has a trust table and unlike ATSN [5], the sensor node just has a trust rating value. In our framework, a node has several trusts rating value. If a sensor node just does a simple thing, which means the sensor just one kind of event happened to it, then just one trust rating to it. The number of trust rating in a sensor node depended on the number of event in sensor node.

Figure 1 depicts the building blocks of event-based trust framework model in WSNs

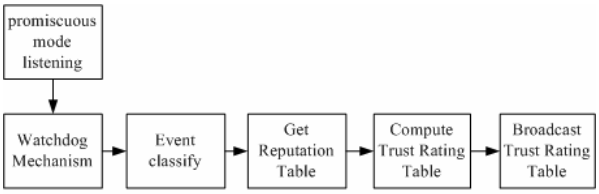

Figure 1: System Architecture

The agent node uses watchdog mechanism in promiscuous mode to listen the channel, the agent node can monitor different event happened in its neighbor sensor nodes. After that, the agent node classifies all the events and uses event function get the reputation table of a sensor node. This reputation related to event function which we will describe in detail in section 3.2. After get the reputation table, the agent nodes compute the trust rating table based on reputation table and event certainty. Finally, the agent nodes broadcast the trust rating table of different nodes within its radio range.

3.2 Event and Event Function

In WSNs, a sensor node has several works to do to buildup a self-organization network, such as data collection, data route, neighbor found, time-synchronization and location report. A senor node should do a series events, and the sensor node has different performance when doing these different events. Some is good performance and some is bad performance. We call them positive output and negative output. And on other hand, some event is emergent or important, some is unimportant event. We use event function to distinguish them. We describe them below.

Definition 1: Event E happened in sensor nodes.

Let $E=\{e_1,e_2,e_3,....e_n\}$ (1)

Because different nodes have different performance, we use Event function to score the sensor nodes.

Definition 2: Event function.

$$F=\{F(e_i)|\ \forall e_i \in E, F(e_i) \geq 1, F(e_i) \in N\} \quad (2)$$

In definition 2, if $F(e_i)=1$, for $\forall e_i \in E$, then it get the result of [1, 5].

When a sensor node does an event, for e_i, the sensor node can get two different outputs to other sensor nodes. One is negative, the other one is positive. We use p_i refer to positive outputs value; n_i refer to negative outputs value, respectively. All of these p_i and n_i satisfy the following formula.

$$p_i = F(e_i) \text{ or } n_i = F(e_i),\ \bigcup_{i=1}^{n} p_i \bigcup_{i=1}^{n} n_i = F \quad (3)$$

$<p_i,n_i>$ is binary event for a certain event e_i of sensor node.

3.3 Reputation Space

RFSN [1], define trust as $T=\frac{p+1}{p+n+2}$, which ignore the uncertainty event probability. And in ASTN[5], Chen et al use a triplet in $[0, 1]^3$ to evaluate trust metrics. But in ATSN [5], the author didn't tell the different event to evaluate the trust rating of the sensor. If the malicious sensor node has good performance on unimportant event, then the malicious node gets high trust rating. But when there is an emergent event happened in WSNs, other sensor nodes cannot detect the malicious node, and as usually, the other sensor will cooperate with malicious node. So, in ATSN[5], the scheme can be attacked by this kind of attacker.

In section 3.2, we get $<p_i,n_i>$, the binary event for a certain event e_i of sensor node, which is positive outcomes and negative outcomes for the event e_i. Accordingly, we model the reputation table space as $RS=N^+ \times N^+$.

Definition 3: Define reputation space of event e_i

$$RS(e_i)=\{<p_i,n_i>|t_i=p_i+n_i;p_i=F(e_i) \text{ or } n_i=F(e_i)\ \forall e_i \in E\} \quad (4)$$

In our event-based trust framework, a sensor node has more that one reputation space. Each event has a reputation space store in agent nodes memory.

3.4 Certainty of Event

Let x_i be the probability of a positive outcome of the event e_i. The posterior probability of $<p_i,n_i>$ is the conditional probability of x_i in given $<p_i,n_i>$ [3].

Definition 4: The posterior probability $P_{<p_i,n_i>}(x_i)$:

$$P_{<p_i,n_i>}(x_i)=P(x_i|<p_i,n_i>)=\frac{P(<p_i,n_i>|x_i)P(x_i)}{\sum P(<p_i,n_i>|x)P(x_i)} = \frac{(p_i+n_i+1)!}{p_i!n_i!} x_i^{p_i}(1-x_i)^{n_i} \quad (5)$$

RFSN[1] Probability theory models the event $<p,n>$ by trust, $T=\frac{p+1}{p+n+2}$, which ignore the uncertainty event probability. We will show if the certainty of event equal to 1, we get the result as RFSN. And we will show if for $F(e_i)=1$, for $\forall e_i \in E$, which means $p_i=1(\text{or } n_i=1)\ \forall e_i \in E$, then we will get the result of ATSN [5] if the sensor node just has one reputation space.

Definition 5: Certainty of the event e_i, $<p_i,n_i>$ [3].

$$c_i(p_i,n_i)=\frac{1}{2}\int_0^1\left|\frac{(p_i+n_i+1)!}{p_i!n_i!}x_i^{p_i}(1-x_i)^{n_i}-1\right|dx \quad (6)$$

Throughout, p_i, n_i, and $t_i=p_i+n_i$ refer to positive outputs value, negative outputs value, and total outputs value, respectively.

3.5 From Reputation Space to Trust Space

Instead of modeling the binary events of event e_i by an events pair $<p_i,n_i>$, we model the trust by (pt_i,nt_i,ut_i). pt_i, nt_i and ut_i refer to positive trust, negative trust and uncertainty of the event e_i, respectively.

Definition 6: Let $T_i(<p_i,n_i>)=(pt_i,nt_i,nt_i)$ be the transformation from binary event $<p_i,n_i>$ to trust rating (pt_i,nt_i,ut_i), where pt_i, nt_i and ut_i satisfy the following conditions:

$$\begin{cases} pt_i(p_i,n_i)=c_i\dfrac{p_i+1}{p_i+n_i+2} \\ nt_i(p_i,n_i)=c_i\dfrac{n_i+1}{p_i+n_i+2} \\ ut_i(p_i,n_i)=1-pt_i(p_i,n_i)-nt_i(p_i,n_i) \end{cases} \quad (7)$$

Where c_i is defined in Definition 5. c_i lies in [0, 1], with c_i = 1 and c_i = 0 indicating perfect knowledge and ignorance of a series of events e_i done by the sensor node, respectively. If $F(e_i)=1, \text{ for } \forall e_i \in E$, which means $p_i=1$ or $n_i=1$, for every event e_i. Then we get the result of ATSN [5], and if for every event e_i, $c_i=1$, then we get the result of RTSN[1].

4. Trust Aging and Trust Distribution

In our event-based trust framework model, every agent node uses a fixed time window function to record the traffic data and classify the event. The agent node has different reputation value of the event for sensor nodes within its radio range in each time window. It is intuitive to imagine that the recently obtained information should be given more weight. The most commonly used technique that addresses this issue is to introduce a forgetting factor [4]. Our framework model uses the following equation to update the trust rating of sensor nodes:

$$T_{sti}=\alpha \bullet T_{sti}^{curr} \oplus (1-\alpha) \bullet T_{sti}^{newg} \quad (8)$$

Where α is an aging factor, it can take a value in the interval [0, 1]. T_{sti} is the trust rating of node s about event e_i, and it was stored in the memory of node t. The value T_{sti} is a weighted sum of two components. The first part describes the sensor node's trust rating already present in the trust table of sensor node about event e_i. The second part reflects contribution of sensor node's new trust rating value about event e_i in fixed time window. As a sensor node's previous trust rating is also considered, the evaluation of trust rating will be more consistent and seamless. The operator $\oplus$ defined in ATSN[5].

In the following section, we will discuss the trust rating distributed by agent node. The distribution process can be done in two ways: (1) Broadcast method in fixed time window, and (2) Trigger method. And it was described by Algorithm 1.

Algorithm 1: Trust Rating Distribution Mechanism

```
while True
For all the nodes s and t in the agent node radio
range
    For event e1 to en
    Agnet node gets the binary event <pi,ni>
    Agent computes the trust rating Tsti;
      If (Tsti) < a certain value
        Break;
      End if
    End for
The agent broadcasts the trust rating Tsti;
End for
  If the time is the begin of window time
    The agent broadcasts all the trust rating Tsti;
    End If
End While
```

In algorithm 1, at first, the agent nodes get the reputation of every event in its neighbor node. Then the agent node compute the trust rating by formula (7),if there is a trust rating below the predefined threshold, then the agent node makes a break and stop computing the others reputation value and trust rating. The agent node broadcast the current trust rating which below the threshold. If has no trust rating below the predefined threshold, then the agent node broadcasts the trust rating in the beginning of next window time.

In our trust framework, the agent nodes do not store the trust rating. They listen to the channel and compute the trust rating, and then broadcast the trust rating. And the sensor node within the agent node's radio range will receive the trust rating and update the trust rating by formula (8). The sensor used the trust rating to make a decision whether to cooperate or un-cooperate with current neighbor nodes in its radio range.

5. Simulations

Our simulator is composed of the following modules: Wireless sensor networks, traffic data, the sensor nodes, the agent nodes, intruder nodes, events generator. The intruder nodes' behavior can good or bad at any moment to different events. The intruder nodes except take on-off attack [5], and take the following attack: The intruder cooperates with the node x_i, when the intruder executes event e_i, its performance well; when the intruder executes event e_j, its performance bad.

5.1. Network Setup

We have discussed the event-based trust framework model in section 3 and, trust rating aging and trust distribution in section 4. We consider a network scenario where the sensor nodes and agent nodes are scattered randomly to monitor the object of a terrain.

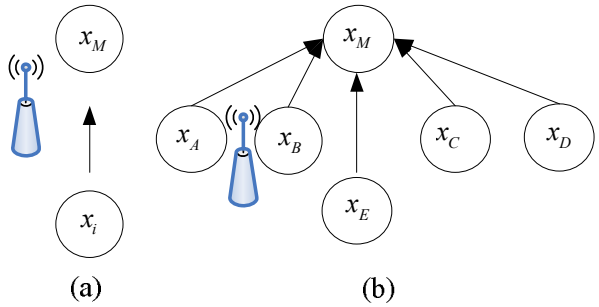

Figure 2: Network Setup

Case (a): We consider node x_i and x_M, shown in Figure 2(a). The node x_M is a malicious node. The node x_M executes several events for the node x_i, such as date collection, packet forward and time-synchronization. The node x_M does well in date collection and time- synchronization, but does badly in packet forward.

Case (b): the node x_M is a malicious node. In the begin of several window times, the node x_M performs well for these nodes x_A, x_B, x_C in every events, and it does badly to these nodes x_D, x_E. And we suppose that the node x_M just does one events. And the event is delivering packet for them.

Our agent node use window function to monitor the behavior of its neighbor sensor nodes. The time is divided into slices; the window function takes several slices time. We set two slices one second and one window time has ten slices. The agent node broadcasts the trust rating at each end of window time. If the agent find the trust rating below the pre-defined trust rating, the agent node makes a break and to distribute the trust rating. The agent node doesn't save the trust rating of these sensor nodes within its radio range. The agent nodes only need to monitor and compute the trust rating. The sensor nodes need to storage the trust rating which distributed by the agent node. And the sensor node updates the trust rating by equation (8).

5.2 result and analyses

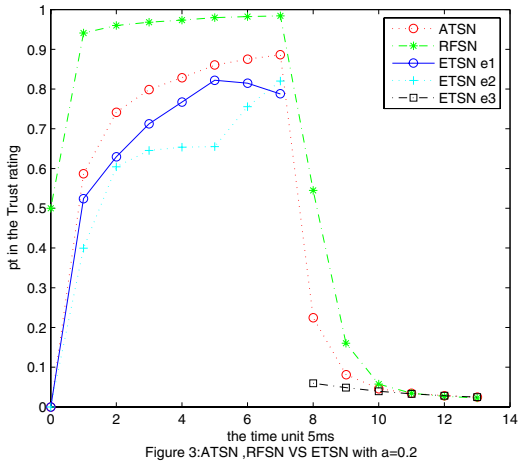

Figure 3:ATSN ,RFSN VS ETSN with a=0.2

In Figure 3, that is the simulation result of Figure 2 (a). In the first 7 slices, the node x_M does well in date collection (event e_1) and time-synchronization (event e_2), so the trust rating of event e_1 and event e_2 are high, the node x_i can cooperate with node x_M. But the trust rating of event e_3 (delivers packet for node x_i.) is low. In our ETSN, the node can continue cooperate with node x_M in the event e_1 and event e_2.But both ATSN and RTSN cannot cooperate with the node x_M due the low trust rating. Our ETSN is more suitable for WSNs.

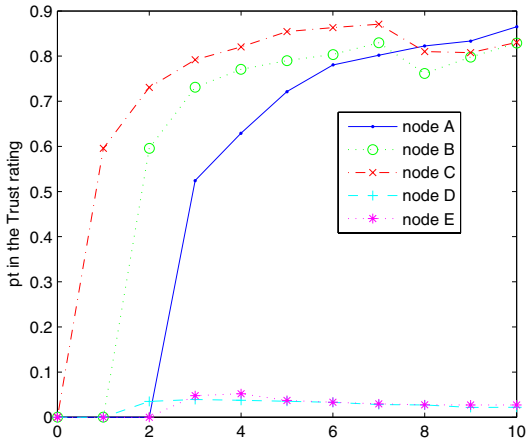

Figure 4: Different trust rating

In figure 4, that is the simulation result of Figure 2 (b).From figure 4, we can get that the node x_M has different trust rating to its neighbor nodes. These nodes $x_{A,}x_{B,}x_C$ can cooperate with the node x_M due to its trust rating. But these nodes $x_{D,}x_E$ don't cooperate with it. Our ETSN can also detect On-Off attack [5]. These neighbor nodes can decide whether cooperate with the node x_M according to its own trust rating.

6. Conclusion

In this paper, we propose Event-based trust framework model to enforce the security of WSNs. The agent nodes monitor the behavior of sensor nodes within its radio range to distribute the trust rating. The system is distributed and we don't need the second-hand information to build trust system. Our ETSN scheme is more suitable for trust system in WSNs due to its different event-related trust rating. A sensor node has several trusting rating in WSNs. It can be used in large scale wireless sensor networks. With the growing importance of sensor network applications, our scheme helps to provide a more accurate guarantee along with cryptographic mechanisms of the actual time to detect the malicious node in different event in WSNs.

7. Acknowledgement

This paper was supported by Shanghai Normal University, the project ID is: SK200705. And the research work in this paper was also sponsored by the expenditure budget program of Shanghai Municipal Education Commission (2008108).

References

[1]S. Ganeriwal and M. Srivastava. "Reputation-based framework for high integrity sensor networks". In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), pp. 66-77, Oct 2004.

[2]Haiguang Chen, Huafeng Wu , Xi Zhou , Chuanshan Gao, Reputation-based Trust in Wireless Sensor Networks ,2007 International Conference on Multimedia and Ubiquitous Engineering (MUE2007) pp. 603-607, April , 2007,Seoul, Korea.

[3]Haiguang Chen, Huafeng Wu , Xiu Cao , Chuanshan Gao Trust Propagation and Aggregation in Wireless Sensor Networks .The 2007 Japan-China Joint Workshop on Frontier of Computer Science and Technology (FCST-2007), Wuhan, China, 1-3 November 2007

[4]A. Jsang and R. Ismail. The Beta Reputation System. In Proceedings of the 15th Bled Electronic Commerce Conference, June 2002.

[5]Haiguang Chen, Huafeng Wu , Xi Zhou, Chuanshan Gao Agent-based Trust Model in Wireless Sensor Networks 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2007) PP 119-124,July 30 - Aug 1, 2007 Qingdao,China.

[6] F. Ye, H. Luo, S. Lu, L. Zhang. "Statistical Enroute Detection and Filtering of Injected False Data in Sensor Networks". In Proceedings of IEEE Infocom, 2004.

[7]J. Deng, R. Han and S. Mishra. "The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks". In the Proceedings of IPSN, April, 2003.

[8] C. Karlof, N. Sastry, D. Wagner. "TinySec: Link Layer Encryption for Tiny Devices". To appear in ACM SenSys, 2004.

[9]S. Ganeriwal, R. Kumar, C. C. Han. S. Lee, M. B.Srivastava. "Location & Identity based Secure Event Report Generation for Sensor Networks". NESL Techanical Report, May 2004.

[10]Haiguang Chen, Peng Han ,Bo Yu, Chuanshan Gao "A New Kind of Session Keys Based on Message Scheme for Sensor Networks". The Seventeenth Asia Pacific Microwave Conference (APMC 2005) Suzhou , China , Dec. 4-7, 2005

[11]A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks", IEEE Wireless Communications, vol. 11, no. 1, pp. 48-60, Feb 2004.

[12]Haiguang Chen, Peng Han, Xi Zhou, Chuanshan Gao. Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks. Will be appeared in Pacific Asian Workshop on ISI (PAISI 2007) Chengdu,China, April, 2007

[13]M. Blaze, J. Feigenbaum, and J. Lacy. "Decentralized Trust Management". In Proceedings of IEEE Conf. Security and Privacy, Oakland, California, USA,1996.

[14]S. Buchegger and J.-Y. Le Boudec. "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks)".Proceedings of MobiHoc 2002, Lausanne, CH, June 2002.

[15]S. Buchegger and J.-Y. Le Boudec. "Self-policing mobile ad-hoc networks by reputation systems". IEEE Communications Magazine, July 2005.

[16]D.Estrin L.Girod, G.Pottie, M.Srivastava, "Instrumenting the World with Wireless Sensor Networks," IEEE ICASSP 2001, p.2033-2036, vol.4, 2001.