Entropy Trust based Approach against IP Spoofing Attacks in Network

Sovan Bhattacharya
School of Education Technology,
Jadavpur University,
Kolkata-32

Arnab Ghosh
School of Education Technology,
Jadavpur University,
Kolkata-32

ABSTRACT

Designing and architecture of Trust model in WSN is now a days research challenge. Trust is important in wireless networks because collaboration and cooperation among nodes and critical towards achieving the system's goals, such as routing reliability. IP-spoofing attacks remain one of the most damaging attacks in which a router replaces the original source IP-address by a new one. This paper present a novel approach using Entropy inference model that evaluates the trustworthiness of an access router and distributed router with regards to forwarding packets. The trust values for the Group router is computed by a judge router that samples all traffic being forwarded by the access router. The trust values for the access router and distributed router are computed by distributed router and ingress/egress router respectively. The simulation results to detects malicious access routers and malicious distributed routers.

KEYWORDS

Trust, IP-spoofing, Group Routing System, Access Router, Distributed Router, Entropy Inference**.**

1. INTRODUCTION

Computer networks are now widely used in many promising application areas, including military surveillance and environment monitoring. The sensor nodes cooperate to perform the target task such as localization and tracking, which they trust one another and work well during the cooperation process. Tools to detect and mitigate attacks have become more and more advanced; however, there are some attacks that have not been effectively addressed. Two of those attacks are the denial of service (DoS) attacks and Impersonation attacks. In [13] a distributed DoS (DDoS) attack, the assault is coordinated across many hijacked systems (*zombies*) by a single attacker (*master*). Techniques that detect DoS also apply to DDoS. The malicious workload in network-based DoS attacks comprises network datagrams. DDoS program must be deployed on one or more compromised hosts before attacks are possible. The several mechanisms are available to mitigate DoS/DDoS attacks and impersonation attacks so difficult to defend is that attacks use spoofed packets.

IP-spoofing: In this attack an intermediate node changes the source address of an IP-packet. Intermediate nodes in a path use trust to isolate the node that might modify the source IP.

Besides malicious attacks, sensor nodes are also vulnerable to system faults. Non-malicious behaviour such as malfunctioning of radio/sensors can also result in the generation of bogus data, bringing equally detrimental effects to the functioning of the network. Attacks that use IP-spoofed packets can easily defeat all the defences that detect attacks based on the source of a packet, such as packet filtering approaches to stop DoS attacks [14]. Thus, an attacker can gain access to services or resources by modifying the source addresses of packets accordingly. While there are several approaches proposed in the literature to address the IP spoofing attacks, there is still a strong need for more effective approaches.

Trust is a useful incentive for encouraging nodes to collaborate. Nodes who refrain from cooperation get lower trust values and will be eventually penalized because other nodes tend to only cooperate with highly trusted ones. So far, most detection mechanisms assume that the IP-spoofed packets are created at the routers or end-host level. With the advent of more sophisticated attacking tools, it has become much easier to take control over *access routers* (AS) and *distributed routers* (DR) that were before thought to be protected.

In this paper proposed Entropy trust-based approach to detect and mitigate an IP-spoofing attack that originates at the access-router level and distributed-router level. The *judge router* calculates the trustworthiness of all Group routers connected to it by applying a Entropy inference model on the number of observed IP-spoofed packets. All access routers are required to send a copy of every packet they forward to the judge router. The mechanism against IP-spoofing attack should have the following characteristics:

- It should have low false-positive and false-negative rates.
- It should have a minimum impact on the network's performance when no attack is occurring.

The remainder of this paper is structured as follows. The related work is discussed in section 2. Our proposed approach is presented in section 3. Simulation results are presented in section 4. In Section 5, we present conclusions and future work.

2. RELATED WORK

Many activities in the human society are based on trust mechanism. Trust in the human society has become the basis of human beings' communications, work and lives. People gradually form the standard of mutual trust, and they always The trust mechanism in the human society was first introduced to security field in computer science. Nowadays, establishing trust for WSNs is still an open and challenging problem.

In [5], trust is defined as a level of confidence of an entity that stable routes are established through the highly trusted nodes having sufficient demonstrate that TETO can secure the

payments and trust calculation and significantly improve route stability and thus the packet delivery ratio.

Trust has been successfully used to performs safe routing [11, 17], or to establish authenticity [16]. In [1, 17], Nguyen et al. presents a Bayesian approach similar to this paper; the main difference is that their focus is to provide better quality of service and to mitigating IP-spoofing attacks. In [11], Sun et al. mathematically model two trust approaches to detect and respond to packet dropping attacks based on a binomial distribution. In [16], trust is modelled as a graph , where the nodes represent entities and each edge represents a trust relation between two entities.

In [6], Matthew J. approach that establishes reputation –based trust among sensor nodes in order to identify malfunctioning and malicious sensor nodes and minimized their impacts on applications. In [4], Yonghong Wang, approach formal trust model for multi-agent system. In [7], Nidal approach, to overcome the weakness of Watchdog and introduce our intrusion detection system called ExWatchdog. In [8], proposed to calculation of trust of individual nodes using both Direct and Indirect Trusts and thereby use the calculated trusts for determination of the different route trusts (RTs) to the Base Station. In [10], propose the LT Code IP Trace back scheme to reconstruct the attack graph and find the source of attacker.

3. PROPOSED APPROACH

In [1, 15] the authors introduce a reputation framework for high integrity sensor networks based on Bayesian formulation. The existing approaches against IP-spoofing attacks assumed that within an Group Router , AS and DR are the attackers and that all the routers are well-behaved entities. Our proposed approach address IP-spoofing attacks at the access router level and distributed router level.

3.1 Group Router Architecture

In our approach we introduce a Group Router (GR). In GR is define as a set of interconnected hosts, routers, hubs, etc. that can be administered by a single organization. The architecture of GR is shown in Figure 1.

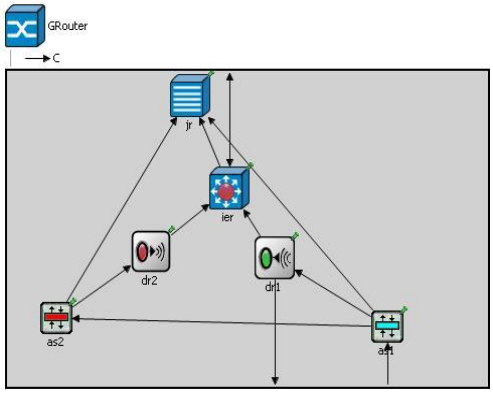

Fig 1: A set of end hosts is connected to access router(AS) and distributed router(DR). within every GR there is a judge (JR), which is in charge of evaluating trustworthiness of GR. AS, forwards traffic to the ingress/egress routers (IER) through the distributed router (DR) and DR also send packet to the end hosts. Note that the IER router, also connect to JR.

In this Group Router, where AS received the packets from end hosts and send to the IER via DR router. AS router also send a one copy of the packet to JR, who perform the packet analysis. Adding a judge router does not significantly increase financial cost nor increases overhead in this network. IER router is connected to another group router IER, for collecting information. IER router send all non-spoofed packet to the JR. In the GR, there is present malicious access router (AS2) and malicious distributed router (DR2). In AS2 received the packets from AS1, send it to DR2 and send one copy of packets to JR. DS2 is send packets to the IER. In order to better utilize JR, some functionalities, such as packet-based attacks analysis, trace back approaches, etc. that are currently being performed at the distribution or core routers could be move to JR.

3.2 The Cases of Threat Detections.

In scenarios there is different types of possible IP-spoofed attacks is presents. In the malicious access router and malicious distributed router both are generates the IP-spoofed packets and tries to avoid detection.

In the Group Router two access routers are presents, AS1 and AS2. AS1 act as non-malicious access router and another AS2 act as a malicious access router. One judge router, JR; one ingress/egress router, IER; two distributed routers, DR1 and DR2. DR1 acts as non-malicious distributed routers and another DR2 acts as a malicious distributed router. AS1 and AS2 both directly connected to JR; AS1 and AS2 are connected to DR1 and DR2 in simultaneously. In DR1 and DR2 both are connected to IER. IER is connected to JR. IER in GR also connected to another GR , IER.

In this approach it is required that when an access routers (AS1 and AS2) receives a packet it forwards the original packet to the distributed routers, (DR1 and DR2), and a copy of that packet to JR through the directly connected links. It is also required that when an ingress/egress router (IER) receives a packet coming from within the AS via DR it forwards the original packets to the next ingress/egress router and a copy of that packet to JR.

Describe in different cases in below:

Case 1: *AS2 and DR2 both are non-malicious*

In this case both AS2 and DR2 both are non-malicious then all the packet are non- spoofed. AS2 send all the packet to DR2 and one copy to JR. DR2 is received packets from AS2, check and count the total number of non-spoofed packet and calculate the AS2 Trust value. In DR2 is send all non-spoofed packet to IER router. IER received packets and count the total number of non-spoofed packet number, then calculate the DR2 Trust value.

Case 2: *AS2 non-malicious but DR2 malicious*

In this case AS2 is non-malicious router. Assume AS2 received y number of packets. It is non-malicious then send y number of non-spoofed packet to JR and DR2. DR2 received y number of packet and count the y number of packet are non-spoofed, then calculate the Trust value of AS2. Assume, DR2 is malicious and it spoofed n number of packets, send y number of packets to IER. IER received y number of packet, check and count n number of packet is spoofed, (y-n) number of packet is non-spoofed, then calculate the Trust value of DR2.

Case 3: AS2 malicious but DR2 non-malicious

In this case, AS2 is malicious. Assume, AS2 received y number packet and spoofed the n number of packet, then y

number of packet send to JR and DR2. After that DR2 received the y number of packet and check and count n number of packet is spoofed,(y-n) is the non-spoofed packet. DR2 calculate the AS2 Trust value. DR2 is non-malicious, (y-n) number of non-spoofing packet is send IER. In IER received (y-n) non-spoofed packet and calculate DR2 Trust value.

Case 4: *AS2 and DR2 both are malicious*

In this case, both AS2 and DR2 are malicious. Assume, AS2 received the y number of packet and spoofed the n number of packet, send y number of packet to JR and DR2. DR2 received the y number of packet, check and count n number of spoofed packet, (y-n) number of non-spoofed packet. DR2 calculate the AS2 Trust value. Assume, DR2 spoofed m number of packet and send (y-n) number of packet to IER. IER received (y-n) number of packet, check and count m number of packet is spoofed, (y-n-m) number of packet is non-spoofed. IER calculate the trust value of DR2.

3.3 Spoofed Detection Algorithms

In this approach where access router received the packet from end-hosts and it may spoofed the packet or may not spoofed. In the detection algorithm for each iteration first it get the module id of AS and DR routers. For each modular id it analysis the packets which is spoofed or not and in line 6 where received the no of non-spoofed packet and total number of received packet. Then calculate the current Trust value. Gather the past Trust value and then calculate the update Trust value in line 10.

Algorithm for detection_malacious

1. Algorithm detection_malacious(void)
2. module_id is the id elements in AS orDR
3. m =m+1 for each iteration
4. for each module_id
5. for each received packet p
6. packet_analyze(packet p, int module_id)
7. end for
8. taken T_{past} from previous records
9. $T_{current}$=calculate_trust(k,N)
10. T_{update}=updateTrust(T_{past}, $T_{current}$,m)
11. end for
12. end detection_malacious

In the packet analyze phase, if the packet is spoofed then drop the packet otherwise count number of non-spoofed packet and count the total number of received packets in each particular modular id of AS or DR .

Algorithm for packet_analyze

1. Algorithm packet_analyze(packet p, int module_id)
2. Id =module_id element in AS or DR
3. N=N+1 when packet is received in corresponding indivisual Id
4. IF (packet is spoofed)
5. Drop packet
6. Else
7. K=k+1;
8. End IF
9. End packet_analyze

In the calculated Trust phase, taken total number of received packet and total number of non-spoofed packet and calculate current Trust value.

Algorithm for calculate Trust

1. Algorithm calculate_trust (double k, double N) //k is no of non-spoofed packet and N is total number of received packet
2. Double p,Hp,Trust
3. $\mathrm{p} = \frac{\mathrm{k+1}}{\mathrm{N+2}}$
4. $\mathrm{H(p)} = -\mathrm{p}\log_2(\mathrm{p}) - (1-\mathrm{p})\log_2(1-\mathrm{p})$
5. IF(0.5<=p || p<=1.0)
6. Trust=(1-Hp)
7. Else IF(0.0<=p || p<0.5)
8. Trust=(Hp-1)
9. End IF
10. End IF
11. Return Trust
12. End calculate_trust

In the Update Trust phase, take current Trust value, past Trust value and number of iteration, then calculate the Update Trust in line 5.

Algorithm for Update Trust

1. Algorithm updateTrust(double T_{past}, double $T_{current}$, double m)
2. Double w_1, w_2, T_{update}
3. w_1=1-(1/m)
4. $w_2 = 1/m$
5. $T_{update} = w_1 T_{past} + w_2 T_{current}$
6. . End updateTrust

3.4 Trust Calculation

3.4.1 Trust Initialization

Often times, when we want to interact for the first time there is little or no information to determine whether they can trust each other.

3.4.2 Evidence Gathering

The second step on trust-based schemes is to gather evidence in order to refine the trust values that were statically set or learnt from neighbours. By its very nature, trust has its foundations on the previous interactions that a subject has had with the agents under evaluation

3.4.3 Trust Calculation and Decision Making

The third step of trust process is to convert all the evidence gathered into a probability value that can reflect how likely it

is that an agent can perform the activity for which it was trusted. Trust is a relationship established between two entities in order to fulfil a specific action. In particular, one entity trusts the other entity to perform an action. In this work, the first entity that make the assessment called the trustor, the second entity evaluated by the trustor is called the trustee, and the role between trustor and trustee can exchange in specific circumstances.

1) In fact, if the trustor believes that the trustee will definitely perform the action, the trustor fully trusts the trustee and there is no uncertainty; if the trustor believes that the trustee will not perform the action for certain, the trustor does not trusts the trustee and there is no uncertainty. In this case, the trustor has the highest uncertainty.
2) The level of trust can be measured by a continuous real number, referred to as the trust value.
3) Trust is a multi-faced concept. It is subjective and not necessarily systematic.

Notations and Definitions

1) P (<trustor, trustee, action, k, n>) is the probability that trustor expects trustee to fulfill a specific action.
2) H(p) is information entropy of a binary stochastic event.
3) The framework for calculating trust value via single path propagations referred to as trust model.

Trust Model:

More specifically, in [11, 2] Sun el al, claim the entropy is a natural measure for uncertainty. They further argue that for indirect observation different subjects can have different probability values for the same agent and the same actions. In [11, 2] authors use the following equation to calculate trust based on entropy:

$$T = \begin{cases} 1 - H(p) & 0.5 \le p \le 1 \\ H(p) - 1 & 0 \le p < 0.5 \end{cases}$$

Where:

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$$

And, $p = \frac{k+1}{N+2}$

p=P(<truster, trustee, action, k, n>). Let p be the probability that an event occurs, k be the number of successful interaction, n be the number of failures, N ne the total number of interactions (N=k+n), and T be the trustworthiness of the system. In this work, the trust value is a continuous real number in [0,1]. From this definition we can see that when p=1, the trustor trusts the trustee the most and the trust value is 1, when p=0, the trustor distrusts the trustee the most and the trust value is 0. Trust value is an increasing function with p.

Decision Making:

Reputation is assessed as a weighted aggregation of ratings. The trustworthiness value can be used to rank the agents. In this approach agent are simply described as: "an agent is likely to perform the desired activity with a T probability". In [9] authors mixed ranking based and threshold-based approaches. One or more nodes with an individual trust value lower than a threshold

Table 1. Action Performs in Trust values

Trust values	Labels	Nature Of Communication	Action Performs
T=1.0	Very High Trust	Trusted Communication	T=T*1.0
T=>0.8	High Trust	Trusted Communication	T=T*1.0
T<0.80 to >=0.65	Medium Trust	Trusted Communication	T=T*1.1
T<0.65 to >=0.25	Low Trust	Risky Communication	T=T*1.2
T<0.25 to >=0.0	Very Low Trust	Risky Communication	T=T*1.2

3.4.4 Trust Update

The trust update process is closely related to the process of calculating the trust value. The weighted sums of the aggregated positive and negative experiences are used as a record of past evidence. It is common practice to analyze changes in a node's behaviour pattern in order to calculate the probability that undesired results might arise. The equation used is as follows:

$$T_{update} = w_1 T_{past} + w_2 T_{current}$$

Where T_{update}, T_{past}, $T_{current}$ are the updated, the past and the most-recently calculated trust value respectively. w_1 and $w_2$are the weight values, w_1+w_2=1. In general for wireless networks the value of w_2 should always be considerably greater than the value of w_1 (w_2>w_1). In [12] Zhong et al. suggest that w1 should be set to w_1=1-(1/m). Where m is the number of observations over which it may be reasonable to assume that current behaviour will continue.

4. PERFORMANCE ANALYSIS AND COMPARISON

4.1 Simulation & Networks Setup

Here proposed trust model is implemented in the omnetpp-4.2.2.. The research question that we attempt to answer in this section is to what extent the proposed trust-based approach can identify the malicious access router and distributed router that send IP-spoofed packets.

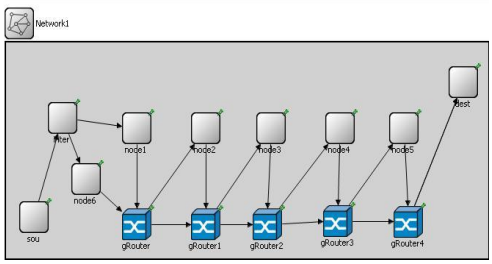

Fig 2: Typical proposed network set up model

To capture the scenarios explained Networks we have implemented our simulation using five Group Router, R1-R5. The behaviour of each of them is defined in each of the simulations.

4.2 Experimental Results

In this simulation where we simulate the 100 no of rounds and take Trust value each individual routers. In Figure 3, shows that comparison between Bayesian trust [1] authors suggest that compare with Entropy Trust values in malicious access router. The x-axis is the no of rounds and the values in the y-axis are trust values of the access routers. We set the trust threshold to 0.8. In this simulation five access router(R1-R5) of them R1 and R5 is low Trusted router but using Entropy Trust value gradually increase after that it saturated but in the Bayesian interference the trust value is more or less same. In figure 3, Here in this graph the router R1 and R5 Trust value is saturated after more number of rounds and it is identified that R1 and R5 are the spoofed router. In the bayesian interference here all router trust value is more or less constant.

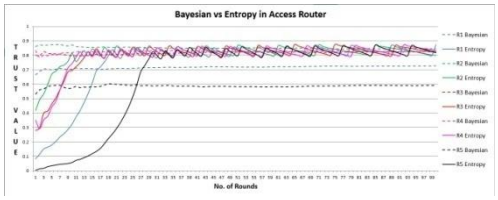

Fig 3: Comparison between Bayesian Trust vs Entropy Trust in the Access Routers (TH =0.8)

In Figure 4, compare between each Access routers Entropy Trust value and Distributed routers Entropy Trust. In this graph Distributed Trust value is greater than Access Router Trust value. Here also apply threshold Trust value 0.8. in this graph shows that access router is more spoofed greater than distributed router because the access router trust value is saturated after more number of rounds than distributed router.

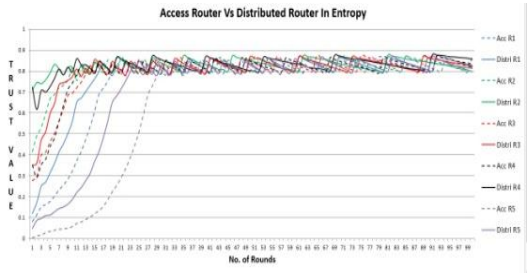

Fig 4: Comparison between Access Routers vs Distributed Routers in the Entropy Trust

In this Figure 5, we compare the Bayesian interference [1] and Entropy interference in each GR. Here set threshold trust value 0.8 . The R1 and R5 in GR trust value is less than other router trust value than it can easily identify that R1 and R5 is spoofed router in Entropy case but Bayesian interference all router Trust value is same then it can't identify that which router is spoofed router .

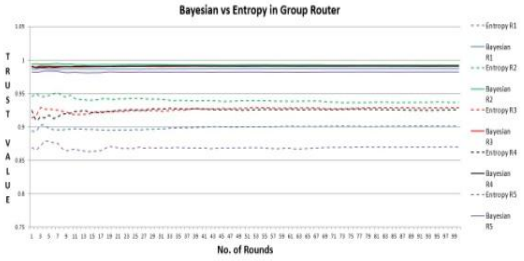

Fig 5: Comparison between Bayesian Trust vs Entropy Trust in the GR (TH =0.8)

5. CONCLUSION AND FUTURE WORKS

In this paper, here presented a Entropy trust-based approach to detect and mitigated IP-spoofing attacks. Here access routers and distributed routers both are malicious or not and compares between them. It can easily identify that which router is spoofed router. To achieved two objectives: our approach takes measure to keep low number of false positive detection; the amount of overhead traffic is reduced to a single packet per access router or distributed routers. For future research, that plan to complements with a methods in Multi-hop Wireless Sensor Networks and used Trust Algebra, that is capable of detecting IP-spoofing performed at the distribution routers as well as access routers detection mechanism to detect and countermeasure rerouting attacks.

6. ACKNOWLEDGEMENT

This paper was fully supported by school of education technology ,Jadavpur University.

7. REFERENCES

[1] Gonzalez, J., Anwar M., Joshi, J., "A trust-based approach against IP-Spoofing attacks," 9th Annual Conf. on Privacy. Trust and Security, Montreal 2011.

[2] Gonzalez, J., Anwar M., Joshi, J., "Trust-based approaches to solve Routing Issues in Ad-hoc wireless Networks: A Survey," International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, Montreal 2011.

[3] Wenzhong, Y., Cuanhe, H., Bo, W., Tong, W., Zhenyu, Z., "A General Trust Model Based on Trust Algebra," Int. conf. in Multimedia Inf. Networking and Security., vol. 1, pp. 125-129, 18-20 Nov. 2009.

[4] Wang Yonghong, Singh Munindar P., "Formal Trust Model for Multiagent Systems," National Science Foundation under grant ITR-0081742, IJCAI-07 1551-1556.

[5] Mahmoud Mohamed Elsalih, Shen Xuemin (Sherman), "Trust-Based and Energy-Aware Incentive Routing Protocol for Multi-hop Wireless Networks," IEEE, 978-1-61284-233-2/11, 2011 .

[6] Probst, M.J., Kasera, S.K., "Statistical trust establishment in wireless sensor networks," Int. Conf on Parallel and Distributed Systems, vol.2, pp.1-8, 5-7 Dec. 2007.

[7] Nasser Nidal, Chen Yunfeng, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks," IEEE, 1-4244-0353-7/07, 2007.

[8] Raha Arnab, Babu Shaik Sahil, Naskar Kanti Mrinal, Alfandi Omar, Hogrefe Dieter, "Trust Integrated Link State Routing Protocol for Wireless Sensor Networks (TILSRP),".

[9] Karthik.N, Sarma Dhulipala.R.V, "TRUST CALCULATION IN WIRELESS SENSOR NETWORKS," IEEE, 978-1-4244-8679-3/11, 2011.

[10] Peng Shih-Hao, Chang Kai-Di, Chen Jiann-Liang, Lin I-Long, and Chao Han-Chieh, "A Probabilistic Packet Marking scheme with LT Code for IP Traceback," *International Journal of Future Computer and Communication, Vol. 1, No. 1, June 2012.*

[11] Sun, Y., Yu, W., Han, Z., Liu, K., "Information theoretic framework of trust modeling and evaluation for ad hoc networks," Selected Areas in Commun., IEEE J., vol.24, pp. 305-317, Feb. 2006.

[12] Zhong, S., Chen, J., Yang, Y.R, "Sprite: a simple cheat-proof, credit-based system for mobile ad-hoc networks, " 22nd Annual Joint Conf. of the IEEE Computer and Communications, vol.3, pp. 1987-1997 vol.3, 30 March-3 April 2003.

[13] Carl, G., Kesidis, G., Brooks, R.R., and Suresh R., "Denial-of-service attack-detection techniques," *Internet Computing, IEEE*, vol.10, no.1, pp. 82- 89, Jan.-Feb. 2006

[14] Hu, Y., Choi, H., Choi, H., "Packet filtering for congestion control under DoS attacks," *Information Assurance Workshop, 2004. Proceedings.Second IEEE International*, pp. 3- 18, 8-9 April 2004

[15] "S. Ganeriwal and M. B. Srivastava. Reputation-Based Framework for High Integrity Sensor Networks. In *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks.*, pages 66–77, Washington, DC, USA, 2004."

[16] Theodorakopoulos, G., Baras, J.S., "On trust models and trust evaluation metrics for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no.2, pp. 318- 328, Feb. 2006

[17] Nguyen, C., Camp, O., Loiseau, S., "A Bayesian network based trust model for improving collaboration in mobile ad hoc networks," *Research, Innovation and Vision for the Future, 2007 IEEE International Conference on*, pp.144-151, 5-9 March 2007