Collusion-resistant reputation-based intrusion detection system for MANETs

Angelo Rossi and Samuel Pierre

Mobile Computing and Networking Laboratory (LARIM), Ecole Polytechnique de Montreal, Montreal, H3T1J4 Canada

Summary

Most intrusion detection systems (IDS) for mobile ad hoc networks (MANETs) are based on reputation system which classifies nodes according to their degree of trust. However, existing IDS all share the same major weakness: the failure to detect and react on colluding attacks. The proposed IDS effectively integrates the colluding risk factor into the computation of the path reliability which considers the number and the reputation of nodes that can compare both the source message and the retransmitted one. Also, the extended architecture effectively detects malicious and colluding nodes in order to isolate them and protect the network. The simulations launched in various MANETs containing various proportions of malicious and colluding nodes show that the proposed solution offers a considerable throughput gain compared to current solutions. By effectively selecting the most reliable route and by promptly detecting colluding attacks, the number of lost messages is decreased, and therefore, offering more efficient transmissions.

Key words:

Intrusion detection system (IDS), mobile ad hoc networks, reputation system, colluding attack, network security

1. Introduction

Cooperation enforcement models for mobile ad hoc networks (MANETs) are based either on trust management mechanisms [1-5] or virtual money [6, 7]. The latter give nodes an incentive to well behave by receiving an amount of virtual money with which they pay other nodes to forward its messages or access distant services. On the other hand, the incentives based on trust entice a node to well behave to keep good relations with its neighbors and thus preventing them to drop messages and become isolated from the network. The degree of trust between nodes is measured through a reputation system by which a node sees its reputation increase after it well-behaved or decrease otherwise. Therefore, the threat of a punishment, resulting in a drop of its reputation, pushes nodes to well behave.

Because every node in MANETs functions not only acts as host but also as a router, the critical operation of forwarding packets may easily be interrupted or corrupted for various reasons, either voluntarily or not. Misbehaving nodes are generally categorized into 3 groups: selfish, malicious and colluding. Selfish nodes main concern is to save as much resource as possible by minimizing the amount of data message forwarding while maintaining a minimum cooperation (above the threshold) to remain in the network. The objective of malicious nodes is to disrupt the network by disseminating false information, overloading neighbors or modifying forwarded messages. Finally, a colluding attack [8] occurs when two or more selfish or malicious nodes collaborate to make an attack without being detected. By observing actions of surrounding nodes, reputation-based solutions can be quite effective against internal active attacks or selfish behaviors. However, to our knowledge very few IDSs consider colluding attacks [9, 10]. Works who do either focus on wormholes attacks [11, 12] or only work for optimized link state routing protocol (OLSR) [13, 14].

This paper proposes a mechanism to detect generic colluding attacks while also thwarting them by extending the pathrater component of reputation based IDS. The research goal is to design an intrusion detection system against colluding attacks in MANETs. In Section 2, a discussion about the strengths and limitations of current IDSs for MANETs is presented. The proposed solution exposed in Section 3 starts by presenting the assumptions and follows with the methods and the algorithms proposed. In Section 4, the experimental results are presented. Finally, Section 5 summarizes the contributions and concludes the paper.

2. Existent IDSs for MANETs

IDSs are composed of 3 distinct modules: detection, filter and reputation. The detection module monitors the behaviors of the surrounding neighbors and sends the information to the filter module which reveals events worth noticing. Finally, the reputation module establishes a score system which rewards or punishes the nodes according to the received events. The authors of [1] are the pioneers of the MANETs IDSs with the introduction of the Watchdog and Pathrater scheme. These two techniques significantly improve the throughput in MANETs in the presence of compromised or malfunctioning nodes.

Manuscript received November 5, 2009
Manuscript revised November 20, 2009

2.1 The watchdog component

The Watchdog component is responsible of monitoring the received messages in promiscuous mode with the purpose of making sure that it has forwarded the message without alteration. Assuming the links are bidirectional (i.e. omnidirectional wireless antennas), when intermediary nodes forward the message to its neighbor, it can also verify that the next hop correctly retransmit the message through the use of the passive acknowledgement. If the message remains unaltered within a specified timeout, the next hop well behaved, else it is misbehaving. According to his behaviors, his reputation will be adjusted. A node can classify a neighbor into one of these 3 classes:

- normal: regroups well-behaving nodes;
- suspect: transitory state for closely monitored nodes;
- malicious: temporary banned and isolated nodes.

Because a node changes state when his reputation reaches a predefined threshold, an attacker can easily exploit the gaps between the thresholds to periodically drop messages. If exploited by several nodes, this simple attack can considerably affect the network throughput. To provide more accurate reputation scores many IDSs propagate indirect observations across the network.

CORE [2], for example, differentiates incoming reputation alerts by grouping them in 3 distinct classes: direct observations, indirect observations (alerts received from distant neighbors) and functional reputation alerts (behavior to accomplish a specific task). The idea is to increase the accuracy by collecting a larger number of alerts, each having a different weight on a node's reputation depending on its type. CONFIDANT [3], which operates similarly to CORE, also accepts indirect observations but their weight is proportional to the reputation of the issuer. Also, in order to reduce the number of alerts crossing the mobile ad hoc network, CONFIDANT only considers negative alerts issued on misbehaviors detections. Note however, the propagation of reputation alerts make these IDSs vulnerable to blackmail attacks.

2.2 The pathrater component

In order to mitigate the effects of misbehaving nodes, the Pathrater selects the most reliable route available instead of simply choosing the shortest route. The reliability of a path is obtained by calculating the average reputation of the intermediary nodes.

The presented approaches suffer from collusion attacks where two or more adjacent attackers that are being part of a route collaborate to drop or falsify messages (assuming no encryption is employed). Fig 1 illustrates the case where nodes B and C collude to modify message M1 without alerting the source. Consequently, the destination D receives a falsified message while source A remains unaware of an intermediary node's misbehavior.

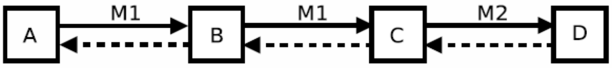

Fig 1. Colluding attack

3. The proposed collusion-resistant IDS for MANETs

3.1 Watchdog and proposed architecture

As depicted in Fig 2, the proposed IDS classifies nodes into seven classes: FRESH, PRIVILEGED MEMBER, REGULAR MEMBER, LITE MEMBER, INSTABLE, SUSPECT and BANNED. According to their rank, each node is treated differently. Splitting the MEMBER class into 3 distinguishes well-working nodes from very reliable ones in which more important responsibilities can be assigned.

When a node discovers new neighbors through route discoveries or source routing analysis in which no reputation have been previously assigned, they are moved to the FRESH class. Starting with a rating of 0, a fresh node is closely monitored by its neighbors for a period of T_{NEW} and is not permitted to send its own messages. After the preliminary observations, the node migrates to LITE MEMBER if its rating respects the minimal threshold for that class. In other cases, it heads to the SUSPECT class and his rating resets to 0.

Nodes that are part of LITE MEMBER can fully participate in the network by acting as a host, an intermediary node and also a source. The rating of a Lite Member node must be between REP_{LITE} and REP_{REG} while the number of ascendant transitions between the UNSTABLE and LITE MEMBER classes below TR_{LITE}.

The most reliable nodes are part of the REGULAR and PRIVILEGED MEMBER classes. They inherit the functionalities of the LITE MEMBER class and ensures the most delicate tasks such as packet rerouting and the participation in local consensuses (see 3.3). By creating 2 classes for reliable nodes, it offers more flexibility with the attribution of important responsibilities while reducing intra-class tolerance abuse. To be part of these classes, nodes must respect the minimum reputation threshold and their number of transitions with lower-rating class must not exceed TR_{REG} or TR_{PRIV}.

When a node's rating goes below REP_{LITE}, it heads to the Unstable transient state where the nodes are temporary placed for reexamination. When entering the UNSTABLE class, their rating is reset to 0 and can only act as hosts and intermediary nodes. After $T_{UNSTABLE}$, their condition is reevaluated. If they are unable to upgrade to the LITE MEMBER class (either because their rating is too low or the number of maximum transitions has been exceeded), then they will be temporarily isolated in the SUSPECT class.

Suspect nodes are temporary isolated from the network by not being able to send, retransmit or receive any messages for a period of $T_{SUSPECT}$. During that time, they will be closely monitored by their neighbors for a period of $T_{INSPECT}$ where any misbehavior will drag the defective node to the permanent dismal list. If no misbehaviors have been noticed, the node will be allowed to reintegrate the network through the UNSTABLE status.

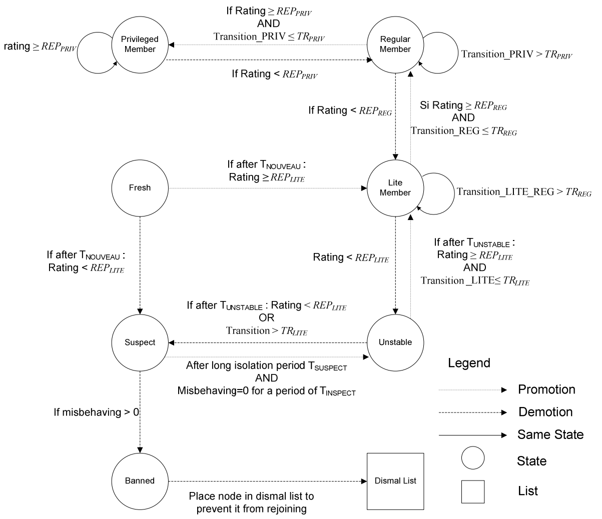
Privileged Member
Regular Member
Fresh
Lite Member
Suspect
Unstable
Banned
Dismal List
rating ≥ REP_{PRIV}
If Rating ≥ REP_{PRIV} AND Transition_PRIV ≤ TR_{PRIV}
If Rating < REP_{PRIV}
Transition_PRIV > TR_{PRIV}
If Rating < REP_{REG}
Si Rating ≥ REP_{REG} AND Transition_REG ≤ TR_{REG}
If after $T_{NOUVEAU}$: Rating ≥ REP_{LITE}
Transition_LITE_REG > TR_{REG}
If after $T_{NOUVEAU}$: Rating < REP_{LITE}
Rating < REP_{LITE}
If after $T_{UNSTABLE}$: Rating ≥ REP_{LITE} AND Transition _LITE≤ TR_{LITE}
If after $T_{UNSTABLE}$: Rating < REP_{LITE} OR Transition > TR_{LITE}
After long isolation period $T_{SUSPECT}$ AND Misbehaving=0 for a period of $T_{INSPECT}$
If misbehaving > 0
Place node in dismal list to prevent it from rejoining
Legend
Promotion
Demotion
Same State
State
List

Fig 2. State machine diagram depicting the operation of the proposed solution

Finally, banned nodes are part of a subjective dismal list maintained by each node individually which forbids them to reenter the network at a later time.

3.2 Pathrater and colluding risk factor

All source routing protocol headers provide rich information on the networks topology. The proposed system collects this information and creates a connectivity table which keeps track of the existent links between nodes. Note that if the assumption that all connections are bidirectional stands, the matrix will be symmetric and only half has to be saved in memory. The following model uses the connectivity table in order to wisely choose the most reliable routes by reducing the risk of colluding attacks.

Table 1. Notations

Sets	
N	Set of all nodes
P	Set of all nodes forming a path from the source to the destination, $P \subseteq N$
I_p	Set of source nodes for path $p \in P, \lvert I_p \rvert = 1$
J_p	set of intermediary nodes for path $p \in P, \lvert J_p \rvert = \lvert P \rvert - 2$
K_i	set of neighbors to $i \in N$ (where $\lvert K_i \rvert$ is the cardinality of K_i representing the number of neighbors of i)
Constants	
TL_iMIN	minimal allowed trust level for $i \in N$
$Nmin_{Ki}$	minimal number of $\lvert K_i \rvert$, $i \in N$
TL_iMIN_{ALERT}	minimal trust level to consider an alert
$ME_i(j)$	maximum tolerance margin between the trust level received from node $i \in K_j$ for node $j \in N$ and the current trust level
Variables	
TLi(j)	trust level of node $j \in N$ from node $i \in N$ point of view
$w_{TLi(j)}$	0-1 variable such that $w_{TLi(j)}$ =1 if and only if $TL_i(j) \geq TL_iMIN, i, j \in N$
n_j	0-1 variable such that n_j =1 if and only if nodes $\lvert K_j \cap K_{j+1} \rvert \geq Nmin_{K_i}, j \in J_p$
w_{ij}	0-1 variable such that wij =1 if and only if $TL_i(j) \geq TL_iMIN_{ALERT}$ and $\left\lvert \frac{TL_j(x) - TL_i(x)}{TL_i(x)} \right\rvert \leq ME_i(j), i, j, x \in N$

The objective

$$max \sum_{j \in J_p} TL_i(j), i \in I_p, p \in P \tag{1}$$

As with other reputation based algorithms, the main objective is to select the path with the highest reputation. However, the computation of the route trust level considers the colluding attack risk factor.

The idea behind the evaluation of the colluding attack risk factor is to determine the number and reputation of available nodes which can detect colluding attacks. Such node must be able to receive messages from an intermediary node $j \in J_p$ and the next intermediary node $j + 1 \in J_p$ in the path $p \in P$. These nodes will be called surveillance nodes. The partial trust level of intermediary node j calculated by the source node i who is seeking the safest route to reach the destination is given by :

$$TL'_i(j) = n_j \sum_{k \in K_j} \sum_{z \in (K_k \cap K_{k+1})} \frac{w_{TL_z(k)} TL_z(k)}{\lvert K_k \cap K_{k+1} \rvert} \tag{2}$$

The first and most important criterion is the respect of the minimal number of surveillance nodes $Nmin_{Ki}$ between the current and the following intermediary node. Once that number is reached, the average of the gathered trust levels about the surveillance nodes is evaluated. In order to demote surveillance nodes with reputation reports below TL_iMIN, trust levels below that threshold are brought down to 0. Note that this strategy requires second hand information to be exchanged among nodes, making this protocol vulnerable to blackmail attacks.

A simpler approach would be for the source nodes i to rely only on their own observations to evaluate the surveillance nodes k and thus eliminate trust level alerts propagation across the network. Equation (3), similar to the previous, shows the algorithm add-on to the pathrater which takes the risk of colluding attacks into consideration.

$$TL'_i(j) = \eta_j \sum_{k\in(K_j\cap K_{j+1})} \frac{w_{TL_i(k)} TL_i(k)}{|K_j \cap K_{j+1}|} \qquad (3)$$

Based on [4, 5] in an environment which permits trust level alerts propagation, the complete trust level can be evaluated with:

$$TL_i(j) = \frac{1}{|K_j|} \sum_{k\in K_j} \left(\frac{w_{TL_i(k)} \times TL_k(j) \times CR_k(k) \times (HMAX_i - H_i(k))}{CMAX_i \times HMAX_i} + \eta_j \sum_{z\in(K_k\cap K_{k+1})} \frac{w_{TL_z(k)} TL_z(k)}{|K_k \cap K_{k+1}|} \right) \qquad (4)$$

By denying trust level alerts forwarding, many simplifications can be applied. First, the factors involving the number of intermediary nodes who forwarded the alerts may be eliminated. Also, because a local consensus (see 3.3) is processed every time a neighbor node changes state, it is not necessary to consider the aging on the alerts. Such concept may still be employed in case some nodes misses the direct alerts from their neighbors, but the probability is generally very slim unless they are overcharged or the network is locally congested.

However, such concept makes it difficult for a node to have an accurate precision on foreign nodes. The introduction of the factor 1/Hi(j) palliates this uncertainty by minimizing the influence of those reputations on the path selection. Of course, this factor must be chosen wisely to avoid selecting the path only on the reputation of the closest next intermediary node.

The pathrater equation (5) is therefore simplified in two terms which can be calibrated by introducing the α and β coefficients. Note that α + β =1 and α, β >0. These coefficients vary in function of the network's security objectives and on available information on the network and remain constant.

$$TL_i(j) = \alpha \frac{TL_i(j)}{H_i(j)} + \beta \eta_j \sum_{k\in(K_j\cap K_{j+1})} \frac{w_{TL_i(k)} TL_i(k)}{|K_j \cap K_{j+1}|} \qquad (5)$$

3.3 Local Consensus

Reputation based IDSs rely on the quality and the quantity of gathered information to select the most reliable path available. Many IDSs such as CONFIDANT therefore permit foreign nodes to spread their direct observations across the network. Such technique definitely increases the quantity of available information, but does not validate the quality and makes it more vulnerable to blackmail attacks.

In order to reduce congestion and increase traffic efficiency, while still maintaining adequate reputation accuracy, nodes initiate the local consensus upon a node migration to another state. By first updating the reputation of the concerned node, all neighbors exchange the reputation of the evaluated node to reach a consensus.

By limiting the propagation of the trust level alerts to their direct neighbors, blackmail attacks will be hard to conduct while still keeping great accuracy locally on nodes reputation. In fact, all gathered reputation alerts are first validated to make sure that the reputation on the concerned node is not too far from the one evaluated with direct observations. Once accepted, it is also pondered with the reputation of source node. However, the lack of information on foreign nodes deeply lowers the accuracy in the path reliability evaluation for the source nodes. Consequently, reliable nodes mandated to select the most reliable routes many will execute many path redirections. The formal model follows.

As a simple prevention against blackmail attacks, only alerts issued from nodes above a specified trust level will be accepted. The variable w_{ij} discards trust level alerts from unreliable sources with a trust level below TL_iMIN. Note that strategy may not be the most accurate. In fact, honest overloaded nodes will usually see their trust level decrease for not forwarding messages and consequently be rejected from local consensuses. On another hand, overloaded nodes will most likely miss a lot of observations on their neighbors and their assigned trust levels will most likely be outdated, therefore acting similarly to blackmail attacks.

As a second attempt to avoid blackmail attacks, gathered trust level alerts must not differ too much from the current node reputation. This criterion is expressed by the second term. Although this article declares the tolerance margin as a constant decided preliminarily by the network administrator, it would be more adequate to be dynamic according to network factors such as the local traffic.

When a node detects a state transition among one of his neighbors, it locally broadcasts a trust level alert specifying the concerned node and his new state. In order to lower the risk of blackmail attacks, only first order observations are exchanged. When a node receives and accepts a trust level alert, it updates the reputation of the concerned node according to equation (6). If this pushes the node to migrate to a different state, it informs his neighbors.

Upon all gathered alerts, the trust level updates are weighted by the reputation of the sources which participated in the local consensus. Because the current node i has a perfect score according to his behaviors, it will have more influence in the update.

$$TL_i(x) = \sum_{j \in K_i} \frac{w_{ij} \times TL_i(j) \times TL_j(x)}{\sum_{j \in K_i}\left(w_{ij} \times TL_i(j)\right)}, x \in K_j \qquad (6)$$

4. Simulation results and analysis

4.1 Simulation design

The experiments have been conducted using Qualnet 4.0 to evaluate the proposed solution by comparing its application layer's throughput with the one of the dynamic source routing (DSR) protocol and the watchdog and pathrater (WDPR) IDS. The chosen primary factors with their respective levels are illustrated in table

Table 2 and the simulation details are showed in table Table 3.

Table 2. Primary factors

Factors		Levels	
Name	**Symbol**	**Name**	**Description**
Number of nodes	N	High	60
		Average	35
		Low	15
Percent of selfish nodes	A	High	35%
		Average	20%
		None	0%
Percent of colluding attackers	C	High	70%
		Average	35%
		None	0%
Mobility	M	High	Low: 2 mps
			High: 20 mps
		Average	Low: 0 mps
			High: 10 mps
		None	Immobile

Table 3. Simulation details

Static factor	Description	
Simulation Time	3 minutes	
Terrain	2kmx2km	
Number of executions per scenario	30 different seeds	
Application	protocol	CBR
	Number transfers	2
	throughput	4096 bps
Node position	Random	
Node direction	Random waypoint	

4.2 Results and analysis

Fig 3 plots the average throughput in an environment with 20% of selfish nodes and 35% of colluding attackers. Results show that the network, exposed to the defined environment, should be composed of at least 25 nodes to get a decent throughput. Because the territory surface is a lot bigger than the wireless broadcasting range, enough nodes should be available in order to find a route to the destination. On the other hand, a high density leads to interferences causing a high collision rate, thus explaining the slight throughput fall when the network totals 60 nodes. Most interestingly, the proposed solution outperforms DSR and WDPR especially in a medium size network. In fact, WDPR and DSR are vulnerable to colluding attacks and thus greatly affected when the number of safe colluding-free routes is limited.

Fig 4 compares the throughput under various percentages of selfish nodes who drop messages at a specified rate. The network has been configured with 60 fixed nodes and no colluding attackers. Results show that the throughput tends to stabilize with the increasing number of selfish nodes for the proposed IDS while decreasing linearly for DSR and WDPR. This can be explained by the rerouting feature which permits highly reliable surveillance nodes to select an alternative path to reach the destination without having the source to wait for his timeout to expire or for an alert to reach him. However, if most surveillance nodes are selfish, they will not reroute the messages and thus the throughput will rapidly decrease.

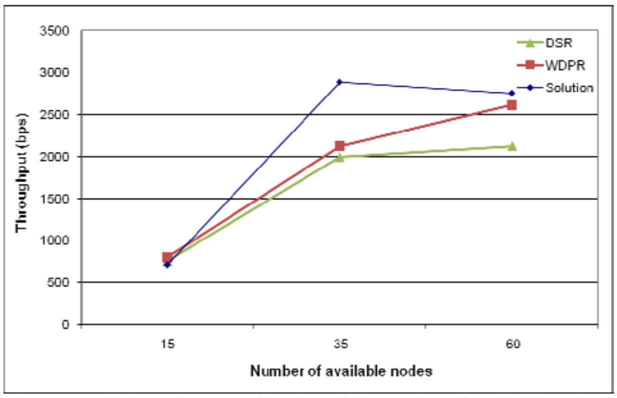

Fig 3. Overall throughput as a function of the number of available nodes in the network (20% malicious and 35% colluding)

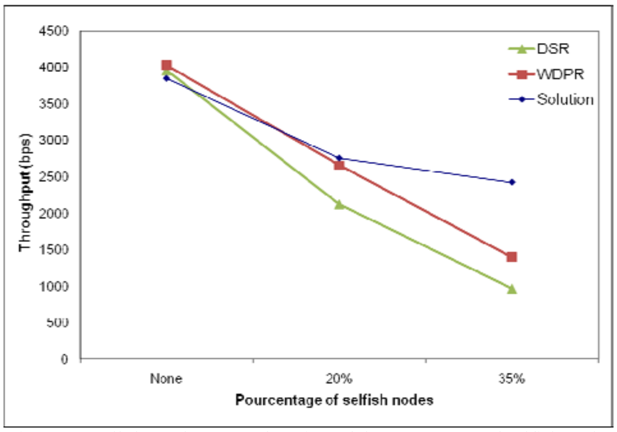

Fig 4. Overall throughput as a function of the percentage of selfish nodes in the network (60 fixed nodes and no colluding attackers)

As expected, Fig 5 shows that the new proposed security mechanisms developed to counter colluding attacks perform almost independently of the ratio of colluding attackers (but below a given threshold). It also shows how WDPR is vulnerable, reaching the same throughput as the DSR protocol with no security mechanisms in place.

One could argue that 70% of colluding attacks is not a realistic scenario. It is important to note that a colluding attack occurs when a colluding attacker precedes a selfish node. Therefore, a presence of 70% of colluding attackers in a 20% selfish acting nodes means that there is a 14% (20% × 70%) risk of a colluding attack to happen. Also, in order to affect the throughput, the colluding attack must occur in a selected path to reach the destination. If the percentage of colluding attackers is too high, the lack of legit surveillance nodes will corrupt our security mechanisms by always selecting the worse path. On the other hand, if the ratio is too low, there will simply not be any colluding attacks in our simulations.

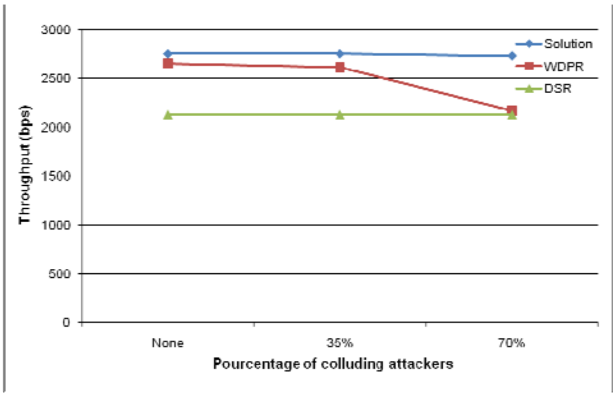

Fig 5. Overall throughput as a function of the percentage of colluding attackers in the network (60 fixed nodes and 20% selfish attackers)

Ad hoc networks are distinguished from other mobile networks by his dynamic topology. As depicted in Fig 6, the delay of convergence for the routing protocol to adapt from sudden route failures and topology changes will inevitably have negative impacts on the network's throughput.

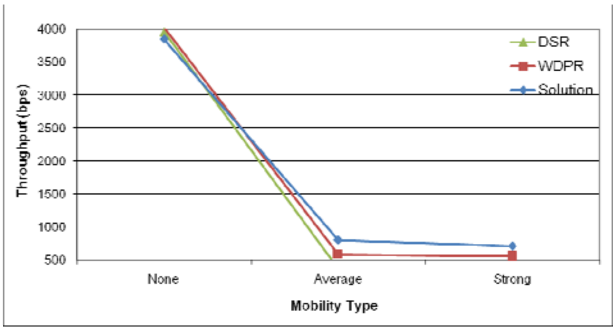

Fig 6. Overall throughput as a function of the nodes mobility (60 mobile nodes and no attackers)

Many factors contribute to the important throughput fall. First, the topology, maintained locally in each node, updates via the reception of route error alerts. However, in such an environment, these error messages may not reach the source and therefore it remains unaware of any changes. Because the functionalities of DSR, from which many IDSs are based on, are dependant on accurate topology information, mobility deeply affects our IDS.

Second, the continuous arrival of new nodes and the departure of neighbors also influence the throughput in two ways. Because IDS' performance is directly related to the acquired knowledge on active nodes in the network, nodes that briefly cross a neighborhood will not get properly classified by his peers. Because new nodes are classified as FRESH, the network will not be able to take advantage of the legitimate nodes in the participation of local consensus or on the detection of colluding attacks.

Fig 7 illustrates how efficient are the new security mechanisms to counter colluding attacks in a very hostile environment with a high colluding attack risk (24.5%). First, the local consensus enables a fast detection of misbehaving nodes. Also, the pathrater selects the safest route based not only on nodes' reputation, but also on the current network's topology to exploit surveillance nodes to react on colluding attacks by retransmitting the lost message via an alternative route.

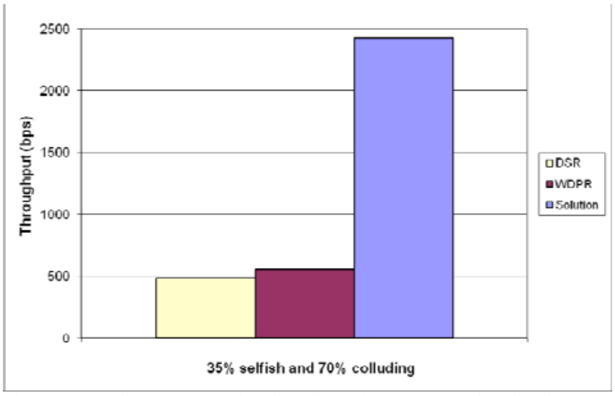

Fig 7. Protocols comparison in a hostile environment (60 fixed nodes, 35% selfish and 70% colluding)

5. Conclusion

In this paper, we have presented a new pathrater algorithm evaluating the reliability of routes not only by the reputation of the intermediary nodes, but also by the number and reputation of available surveillance nodes. Their scope is to monitor transmissions between two adjacent intermediary nodes and detect colluding nodes. If they are part of highly reliable classes, they can also reroute the original message through another path. Also, the local consensus provides an effective reputation evaluation by exchanging alerts with direct neighbors which greatly reduces communication overhead as compared to the schemes that maintain global reputation.

Simulations results show that colluding attacks do not affect the proposed IDS as much as the original watchdog and pathrater. In fact, the overall network throughput remained constant with the arrival of colluding attackers while decreasing drastically with WDPR and DSR.

On the other hand, the practice of choosing the paths with a higher node density will also increase the risk of transmission collisions due to an environment more conducive to internode interferences. It is safe to conclude that the proposed IDS performs better than others in a realistic mobile ad hoc scenario with lightweight traffic.

An interesting future work would be on implementing a dynamic calibration based on statistical analysis to automatically determine optimal threshold values. The adaptative solution will therefore optimize the parameters for the pathrater such as the rating increment and decrement amounts, the timeout delays and isolation times, and the affected weight on the colluding factor. Many QoS attributes of the networks will be gathered and shared among peers to dynamically set these thresholds to their optimal values and consequently increase throughput regardless of the changing conditions affecting the network.

References

[1] Marti, S., T.J. Giuli, and K.B. Lai, M. , Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking 2000: p. 255-265.

[2] Michiardi, P. and R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security. 2002, Kluwer, B.V.

[3] Buchegger, S. and J.-Y. Le Boudec, Performance analysis of the CONFIDANT protocol, in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking and computing. 2002, ACM: Lausanne, Switzerland.

[4] Liu, Z., A.W. Joy, and R.A. Thompson, A Dynamic Trust Model for Mobile Ad Hoc Networks, in Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems. 2004, IEEE Computer Society.

[5] Rebahi, Y., V.E. Mujica-V, and D. Sisalem. A reputation-based trust mechanism for ad hoc networks. 2005. Los Alamitos, CA, USA: IEEE Computer Society.

[6] Zhong, S., Y. Yang, and J. Chen. Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad Hoc Networks. in Proc. of IEEE INFOCOM. 2003.

[7] Xue, Y., B. Li, and K. Nahrstedt, Price-Based Resource Allocation in Wireless Ad Hoc Networks, in Quality of Service — IWQoS 2003. 2003. p. 155-155.

[8] Marshall, J., V. Thakur, and A. Yasinsac. Identifying flaws in the secure routing protocol. in Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International. 2003.

[9] Ghosh, T., N. Pissinou, and K. Makki, Towards designing a trusted routing solution in mobile ad hoc networks. 2005, Kluwer Academic Publishers. p. 985-995.

[10] Ghosh, T., N. Pissinou, and K. Makki. Collaborative trust-based secure routing against colluding malicious nodes in multi-hop ad hoc networks. in Local Computer Networks, 2004. 29th Annual IEEE International Conference on. 2004.

[11] Mahajan, V., M. Natu, and A. Sethi. Analysis of wormhole intrusion attacks in MANETs. 2008. Washington, DC, United states: Institute of Electrical and Electronics Engineers Inc.

[12] Xu, S. and R.V. Boppana. On mitigating in-band wormhole attacks in mobile ad hoc networks. 2008. Piscataway, NJ, USA: IEEE.

[13] Kishore, B.M.N., A. Franklin, and S.C. Ram Murthy, On the prevention of collusion attack in olsr-based mobile ad hoc networks. Proceedings of the 2008 16th International Conference on Networks, ICON 2008, 2008.

[14] Sterne, D., et al. Countering false accusations and collusion in the detection of in-band wormholes. 2008. Piscataway, NJ, USA: IEEE.

Angelo Rossi received the B.Eng. and M.A.Sc. degrees, Ecole Polytechnique de Montréal in 2005 and 2006. He is currently pursuing a Ph.D. degree under a NSERC scholarship in association with Ericsson Canada research labs. His research interests are focused on security in mobile networks with subjects such as intrusion detection systems (IDS) in ad hoc networks and secure protocol designs for the fixed-mobile convergence architecture in 4G networks.

Samuel Pierre received the B.Eng. degree in 1981 from École Polytechnique de Montréal, the B.Sc. and M.A.Sc. degrees in 1984 and 1985, from the UQAM, the M.Sc. degree in 1987 from the Université de Montréal, and the Ph.D. degree in 1991 from École Polytechnique de Montréal. He is currently a Professor of Computer Engineering at École Polytechnique de Montréal, where he is Director of the Mobile Computing and Networking Research Laboratory (LARIM) and NSERC/Ericsson Industrial Research Chair in Next-Generation Mobile Networking Systems. His research interests include wired and wireless networks, mobile computing, artificial intelligence and tele-learning. He is a Fellow of the Engineering Institute of Canada, a senior member of IEEE, and a member of the ACM and the IEEE Communications Society.