Simulation of a Trust and Reputation based Mitigation Protocol for a Black Hole Style Attack on VANETs

Agostino Martorana
Department of Computer Science
Middlesex University London
United Kingdom
Email: xxx

Giuseppe Primiero
Department of Computer Science
Middlesex University London
United Kingdom
Email: G.Primiero@mdx.ac.uk

Jacopo Tagliabue
Tooso
United States
Email: j.tagliabue@tooso.ai

Abstract—From a security standpoint, any VANET (Vehicular ad hoc Network) is a highly flexible network where nodes can freely move and join, with no fixed infrastructure, and thus it is vulnerable to attacks by malicious users. Due to the decentralized and open nature of the wireless system, VANETs are highly prone to various attacks. For many of these kinds of attacks detection is unfeasible, thus making it hard to produce security. It is nonetheless essential to identify network and population properties that can optimise mitigation protocols' deployment. In this paper, we provide a simulation study of a Black Hole stye attack on a VANET and illustrate the use of a previously formally defined trust and mitigation based protocol to contain the attack under well-specified initial conditions.

1. Introduction

MANET (Mobile Ad hoc Network) refers to a self-configuring system of mobile routers, with wireless links to form an arbitrary topology. The mobility of the routers are provided randomly and organized arbitrarily. VANET (Vehicular Ad hoc Network) is the application of MANET structures to vehicles. and roadside unit networks created to enhance transportation systems through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. This kind of systems has various potential applications, such as emergency search and rescue operations, battlefield communication between moving vehicles and/or soldiers or simply traffic control [8], [18].

From a security standpoint, any MANET is a highly flexible network, where nodes can freely move and join, with no fixed infrastructure, and thus it is highly vulnerable to attacks by malicious users. Security of data transmission is the main concern of any MANET. For many of these kinds of attacks detection, is unfeasible, thus making it hard to produce security. Due to their distributed and dynamic nature, such networks are open to several types of threats, including false message propagation. Trust and reputation are among the most used concepts to ensure integrity, reliability and safety of services.

While an increasing literature is available on mitigation protocols for such attacks, the focus on dynamic, reconfigurable networks tend to make these results opaque with respect to conditions of the network when the attack takes place. The present paper simulates a type of attack on a VANET and deploys a trust and reputation model to mititgate it. Contrary to many contributions in the area, we make use of standard network theory analysis to investigate which network properties (like size and topology), which population properties (like proportion of the attackers) and which contextual conditions (like the current content distribution) are optimal to constraint the attack. This allows to set some clear benchmarks for the specific type of attack we consider; the code of our simulation is made available for reproducibility purposes.

2. Related Work

Due to their particular architecture, ad-hoc networks are more easily attacked than wired networks. Two main kind of attacks are usually distinguished [9, p.956]:

- passive attacks: they do not disrupt the operation of the protocol, but try to discover valuable information by listening to traffic;
- active attacks: they inject arbitrary packets and try to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes.

We focus below on active attacks. The most common type, performed due to their easiness, are "Attacks Using Modi-fication": a malicious node disturbs the good operation of an ad-hoc network by announcing better routes (to reach other nodes or just a specific one) than the other nodes. This kind of attack is based on the modification of the metric value for a route or by altering control message fields [9, p.956]. In "Attacks using Impersonation" (spoofing), the malicious node hides its real IP address or MAC addresses and uses another one. As current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. For example, a hacker can create loops in the network to isolate a node from the remainder of the network. To do this, the hacker just has to take the IP address of another node in the network and then use it to announce a new

route (with the smallest metric) to the others nodes. By doing this, he can easily modify the network topology as he wants [9, p.956]. Attacks by "Resource Overuse" indicate the additional use of a resource by a node for any activity other than route finding and maintaining or transmitting data. As mobile nodes may have limited resources in terms of memory, storage, processing power, and battery life, if an IDS involves too much data and computations, then there will be more usage of memory and the processing power, thus disrupting the normal functioning of the network [7, p.388].

Abstracting from the content of the message, several strategies are identified [3, p.345]:

- **Black hole Attack**: in this type of attack, malicious nodes broadcast the message to all the nodes. Diverting all the traffic toward themselves, and without forwarding the data packets to the neighbouring nodes, all the (non-malicious) data packets are dropped;
- **Gray hole Attack**: this attack can be considered as a form of Black hole attack. The malicious nodes drop the data packets for particular nodes for particular period of time in the network. This makes gray hole attacks more difficult to identify as compared to the black hole attacks;
- **Wormhole Attack**: in this type of attack, two malicious nodes from a tunnel and all the data packets received at one location of the network are tunnelled to the other location, in such a way that all the data are resent to the network. The tunnel between two malicious nodes is called a Wormhole. Such attacks prevent any route other than through the wormhole from being discovered;
- **Byzantine Attack**: this type of attack is carried out by intermediate nodes or group of intermediate nodes. Such malicious nodes provide the false routing information and create routing loop as well as forward their data packets to that path which is not optimal which may be harmful to the routing system;
- **Denial of Service Attack**: it prevents the victim from using all or part of the network connections. DOS attack may have numerous forms and are hard to detect. In this type of attack, attacker nodes send the excessive amount of data packet or request to the server so the latter gets busy in testing illegal request and will not be available to other. This attack may degrade the performance of the network since it consumes the energy (Battery Power) of nodes.

Black hole detection has been an active area of research since the 'next hop information' based scheme was proposed in 2002 [4] . But merely a few among the proposed solutions detect collaborative black holes. In [17] the notion of 'Fidelity Table' is introduced. In this model, every participating node is allotted a particular fidelity level, a measure of reliability. Whenever a source node broadcasts a RREQ (Route Request) and holds up, the incoming RREPs (Route Reply) are gathered in its Response Table. If the average

of the fidelity level of RREP sending node (RREPN) and its next hop node (NHN) in the route is found to be over a predetermined threshold, the RREPN (Route Reply Sending Node) is considered as trustworthy. Therefore, on the receipt of multiple RREPNs, the one with the highest fidelity level is selected. However, if multiple nodes have the same fidelity level, the RREPN with the minimal hop count is chosen. Finally, routing is accomplished via the selected path. Upon data receipt, the destination node sends an acknowledgement to the source node within timer. Next, fidelity level of the RREPN is incremented as an accolade for honest routing else that of both RREPN and its NHN is decremented for being collaborative. If fidelity level of a node drops to zero, it is considered as a black hole and the presence of attack is intimated to all using alarm packets. Despite the fact that this method handles both single and collaborative black hole attacks, it involves increased storage overhead, routing overhead, computational overhead and delay. This is because each node should maintain a Fidelity Table and a Response Table that must be updated and exchanged among the nodes periodically [16].

Reputation is complemented by trust models in several VANET models, defined in accordance to their main object: entity-centric [11], [6], data-centric [15], [10] and combined [20]. An overview of the issues related to trust in fixed and mobile ad hoc networks is given in [21], while approaches for trustworthiness and reputation in ad hoc mobile networks are presented, for example, in [5], [2]. The work in [19] offers an analysis that accounts for reputation as a characteristic of message forwarding among vehicles, drivers and other agents: reputation of these agents is based on a descriptive ontology and is used to provide feedback in the system. In [14] we have provided a logic calculus that formally verifies this reputation model by adding a trust function in order to guarantee absence of unsfae behaviours. An interesting way to test the reliability of the model is to simulate an attack.

3. The Attack Scenario

We consider a Black Hole Attack in which a single or multiple nodes are trying to disrupt truthful information in a network by distributing false information. At any point in time the network will have a specific topological configuration and the veichles in it might belong to one of three families (or breed):

- *discoverers*: one or more vehicles in possession of truthful and update data, possibly received by an external network through Internet or a RSU;
- *attackers*: one or more vehicles performing the attack, by distributing false messages within the network;
- *receivers*: the remaining set of vehicles, which have no information, or with information requiring an update.

The action of the discoverers is implemented by the routine defined in Figure 1, where $\_\#turtles$ is the variable

```
to discovery [ _propositionIndex _# turtles ]
  ask n−of _#turtles turtles [ knowProposition _propositionIndex −1 1 ]
end
```

Figure 1. Discovery

```
to spreadKnowledge [ _propositionIndex ]
  ask turtles with [ item _propositionIndex propositions != 0 ]
  [
    let myId who
    let truthVal item _propositionIndex propositions
    ask one−of link−neighbors
    [ knowProposition _propositionIndex myId truthVal ]
  ]
end
```

Figure 2. Message Passing

```
to attack [ _propositionIndex ]
  ask n−of number_attacker turtles with
    [ item _propositionIndex propositions = 1 ]
  [
    set breed attackers
    knowProposition _propositionIndex −2 −1
  ]
end
```

Figure 3. Attack

```
to−report calculateApperceptionValue
[ sourceRanking _propositionRanking _tick ]
  report (1.0*sourceRanking)*(1.0*_propositionRanking)*( _tick *1.0)
end
```

Figure 4. Apperception

name for the subset of nodes generating truthful information (by assumption with truth-value 1).

Message passing is performed by the routine in Figure 2. It requires every agent with a message whose truth value is non-neutral to pass it toone of its neighbors.

By definition, this routine holds for both discoverers and attackers. When an attacker receives the information, for example p on the current outside temperature and road conditions in view of ice and snow, its aim is to flood the network with the information $\neg p$ and to get as many vehicles as possible to distribute it. We implement the attack through the routine defined in Figure 3.

If no protocol is in place to resolve conflicting information transmission, the attack might easily succeed. This is clearly shown by the initial experimental results in Section 5. If a simple majority protocol is used to discern between conflicting data, it might be enough for the attacker to link with a limited number of nodes with low degree of connectivity, in order to flood the entire network.

Several of the work presented in Section 2, introducing trust and reputation methods for VANET attacks, are very limited in their experimental analysis: they do not explicitly express under which conditions (topological, temporal, etc.) are the (often quite promising) results obtained. Our main aim is to investigate whether the trust and reputation protocol presented in [14] is effective in preventing such type of attacks under precise and well specified conditions concerning:

1) the topology of the network at the moment of the attack;
2) the proportion of discoverers and attackers;
3) the ranking of truthful information object of the attack;
4) the state of truthful information diffusion at the moment of the attack.

4. The Trust and Reputation Model

(un)SecureND is a natural deduction calculus defining trust, mistrust and distrust protocols introduced in [13] and extended in [12] with a negation connective. In [14] a modified version has been presented, adapted for a VANET network.

Given $\mathcal{A}$ a set of agents containing vehicles $\mathcal{V}$ and roadside units (RSUs) $\mathcal{R}$, an order $\prec$ between agents is a reputation order. $\mathcal{S}$ denotes a set of services. $\mathcal{C}$ denotes a set of service characteristics, with each element $C^{S_i}_{\vec{n}}$ denoting the set of n characteristics of service S_i. In general, characteristics $C^{S_i}_{\vec{n}}$ of services for each service S_i are associated with an order $\leq$ used to order messages, and for two characteristics $C^{S_i}_{\vec{n}}, C^{S_j}_{\vec{n}}, i \neq j$, there is no order between them. In the present experimental analysis, we limit ourselves to a single message p about a given service with one characteristics. The analysis of the model generalised to multiple messages concerning several characteristics for one service is left to future research.

In the implementation, we translate the order relation $p_i < p_j$ as a fixed absolute ranking value of message p (rank p), which we will assume is shared by all vehicles in each messaging instance, but can assume three distinct numerical values corresponding to low, medium and high. As a further simplification, we assume atomic messages, although the underlying logic (un)SecureND allows for closure under connectives.

For any given message p received from another agent (either vehicle or RSU), a vehicle will collect all the formulas that follow from accepting it. This is called the Feedback Set of an agent with respect to a message. In view of the mentioned simplification, our Feedback Set is always a singleton. The vehicle assigns a value to this atomic formula, using three parameters: a fixed ranking of the source (generated in this model automatically by the topology of the network), a ranking of the message (fixed at some low, medium or high value for each messaging operation) and the time at which the reception of the message occurs (the later the message arrives, the highest its value). We call the resulting value Apperception, see Figure 4.

As a result of working with atomic messages only, the Apeprception of a vehicle for a message is computed by unary factors. Using this value, we define directly the order of reputation for agents, which establishes a higher position for the vehicle whose apperception is greater.

4.1. Network Construction

The original model presented in [19] uses reputation to define a recipient selection protocol: after v_i broadcasts a 'hello' message, if both v_k, v_j receive and accept the message, then v_i has to select a reciepient on the basis of the reputation order between v_k and v_j. Accoridngly, a new profile is built out of v_i and the higher of the two recipients, thus modelling a communication channel.

In the present implementation, given fixed network topologies we assign an agent ranking on their basis. Reputation then is defined by this factor together with message ranking and timing. In particular, we consider the three following main topologies:

- *small-world*: the network is generated according to a power-law, by which each new node has a higher probability to be linked to a node with high in-degree than to one with low in-degree; in this topology, higher in-degree nodes have higher ranking;
- *total*: every node is connected to any other node, and all have the same ranking;
- *random*: edges are randomly distributed, and so is the ranking which reflects the in-degree of each node.

The advantage of fixing the networks and of determining the agent ranking on that basis is to experimentally evaluate the optimal topological conditions for the mitigation protocol. A next step of this protocol evaluation will implement reputation (based on message ranking and timing only) as a criterion for recipient selection.

4.2. Message Passing Protocol

The trust protocol from the logic (un)SecureND enforces a consistency check on message passing. Each valid vehicle profile meets all the requirements and conflicts clauses of all service messages that the vehicle receives. Trust allows to select valid messages among those that are read: if a message is received by a vehicle and it preserves its profile consistency, then it can be trusted. A message readable and trustable by a vehicle can be further broadcast to other vehicles. Mistrust is the protocol acting on conflicting messages: a currently held message conflicting with a newly arrived message is removed from the current vehicle profile and none of its consequences are included; any message consistent with the conflict resolution is trusted by removal of the mistrusted message in the vehicle profile, including any required dependency.

In the present implementation, message passing with consistent information or when the receiving agent is an attacker is unproblematic: it induces respectively acceptance and rejection of the new message. Message passing consistent information to an agent who has no prior information induces a reputation control: information is accepted when coming from a source with higher reputation, while the receiver remains undecided if information comes from a source with lower reputation. A conflict is generated by two

```
to−report  verifyProposition
[ _currentVal _newVal _propositionIndex _breed _currentWho _sourceWho]
  if ( _breed = attackers )
     [ report _currentVal ]
  if ( _currentVal = _newVal)
     [ report _newVal ]
  if ( _currentVal = 0)
  [  ifelse  (sourceApperception >= currentApperception)[ report _newVal ]
    [ report  0 ]
  ]
  if ( _currentVal ! = _newVal)
  [  ifelse  (sourceApperception >= currentApperception)
    [ let  consensus
      neighborConsensus _propositionIndex _newVal sourceApperception
      ifelse  (consensus = false ) [ report _currentVal ]
      [ report _newVal ]
    ]
    [ report _currentVal ]
  ]
]
```

Figure 5. Trust

```
to−report neighborConsensus
[ _propositionIndex _truthVal _sourceApperception ]

  let  total_neighbors_with_opinion  count link−neighbors with
  [item _propositionIndex  propositions != 0
  and item _propositionIndex  apperception > _sourceApperception]

  let  total_neighbors_with_same_opinion  count link−neighbors with
  [item _propositionIndex  propositions = _truthVal
  and item _propositionIndex  apperception > _sourceApperception ]

  if  ( total_neighbors_with_opinion  = 0) [ report false ]
  report  total_neighbors_with_opinion  = total_neighbors_with_same_opinion
end
```

Figure 6. Consensus

contradictory messages, and the profile is valid when such conflicts are avoided. Receiving contradictory information requires again reputation checking: with a source that has reputation at least as high as the receiver, the latter checks with any linked agent with higher reputation than the source; when these show consensus (see Figure 6) with the receiver, the latter does not change its mind, and it does otherwise. See Figure 5.

5. Experimental Results

To experimentally validate our mitigation protocol, we have considered the following parameters:

1) *network topology*: we investigate the optimal topology among small-world, total and random newtorks for the minimization of the attack's effects;
2) *network size*: we consider three main values on this parameter, with networks of $10, 50, 100$ nodes;
3) *message ranking*: a static value at each message passing operation, valid for all agents (both discoverers and attackers), investigated with three different values $0.20, 0.50, 0.80$ corresponding respectively to low, medium, high ranking;
4) *proportion of discoverers*: proportion of agents with truthful information at the beginning of the protocol, investigated with three values $10\%, 50\%, 90\%$;
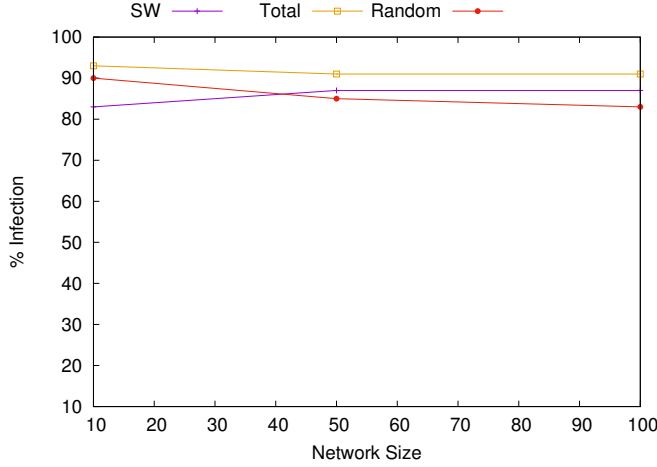
Figure 7. Experiment 1: Attack with 10% attackers/discoverers.

Figure 8. Experiment 2: Attack with 1% attackers and 90% discoverers.

5) *proportion of attackers*: proportion of agents performing an attack, investigated with two values $1\%, 10\%$;
6) *network coverage for attack*: it expresses the coverage of the entire newtork with truthful information when the attack is executed, investigated with three values $20\%, 50\%, 80\%$ corresponding respectively to `low,medium,high` coverage (reflecting an early, intermediate and late attack).

All experiments reported below have been executed on a machine with 7.7 GB of memory, 64bit Ubuntu 17.10 system, NetLogo 6.0. Each configuration has been run for a minimum of 100 times, and for several configurations we have run 10 repetions of 100 runs each.

5.1. First Configuration: Topology and Size

In the first set of experiments, we focus on determining optimal topology and size for our mitigation protocol. We investigate all sizes and topologies while keeping message ranking and network coverage parameters both at a minimum level (respectively 0.20 and 20%).

Our first experiment is executed with a proportion of attackers and of discoverers both fixed at 10%, i.e. with respectively $1, 5, 10$ attackers/discoverers on networks of $10, 50, 100$ nodes. Results are plotted in Figure 7: it clearly illustrates how the attack is highly successful and the protocol has only limited efficacy.

These values tend to decrease sensibly when varying the proportion between attackers and discoverers, in a way which preserves in general the optimality of the topologies. By fixing the proportion of attackers at 1% (in general, this means we are reducing the attacker to 1), but increasing the proportion of discoverers to 90%, we find that the protocol makes the network a lot more resilient to the attack, see Figure 8.

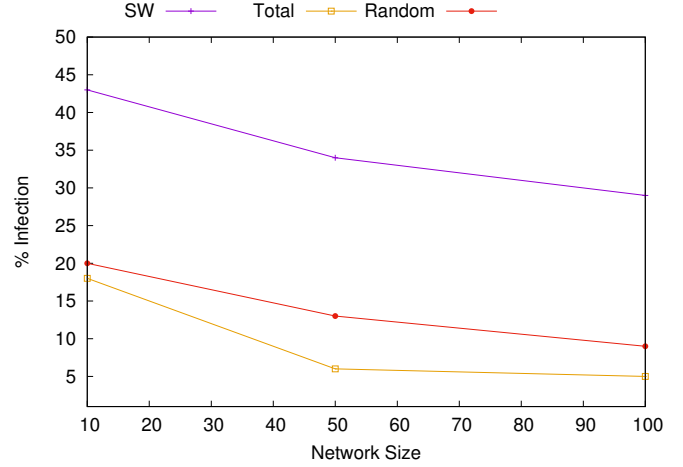Performed – but not reported here – experiments cover several in-between configurations. These initial findings show that, while there is a positive effect intrinsically generated by the network size (the greater the network, the harder to spread the attack), it is sufficient for the attackers breed to cover 10% of the entire population in order to nullify such advantage. On the ohter hand, with a single attacker, size sensibly helps reducing the infection, with a totally connected network presenting the most advantageous setting for the mitigation protocol, followed by random and small-world.

5.2. Second Configuration: Message Ranking

The second set of experiments focuses on how the ranking of the message affects the ability of the protocol to constraint the attack. We show how rising the value of `rankp` from 0.2 to 0.5 in the setting of the first experiment (Figure 7) has an immediate positive effect, bringing a drastic improvement in small newtorks of 10 nodes, and a significant one also in larger configurations, see Figure 9. Further rising the value of `rankp` to 0.8 does not improve these results.

On the other hand, preserving the best results from the first configuration, thus analysing small-world, total and random networks with a single attacker and a proportion of 90% discoverers (i.e. the configuration of Experiment 2 in Figure 8), while rising the level of the variable `rankp` from 0.2 to 0.5 and 0.8, it is possible to show that rising message ranking has no influence in further reducing the infection in all topologies.

5.3. Third Configuration: Network Coverage

The third set of experiments focuses on how the infection is effected when parametrised by the relation between the attack being struck and a percentage of the network having already received truthful data. We show in Figure 10 the results for the setting of the first experiment (Figure 7) modified by rising the value of `network_coverage`
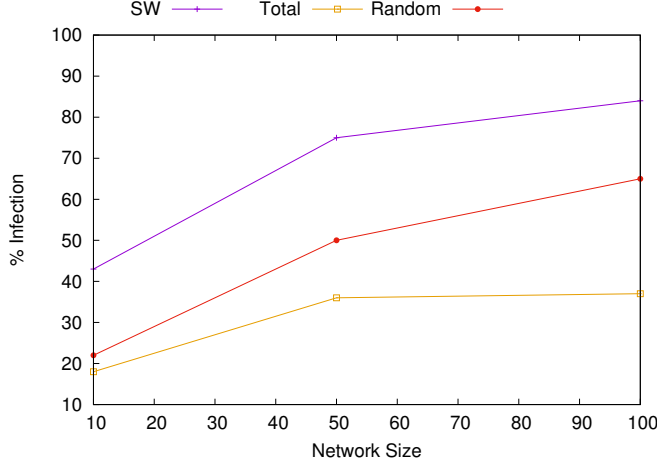
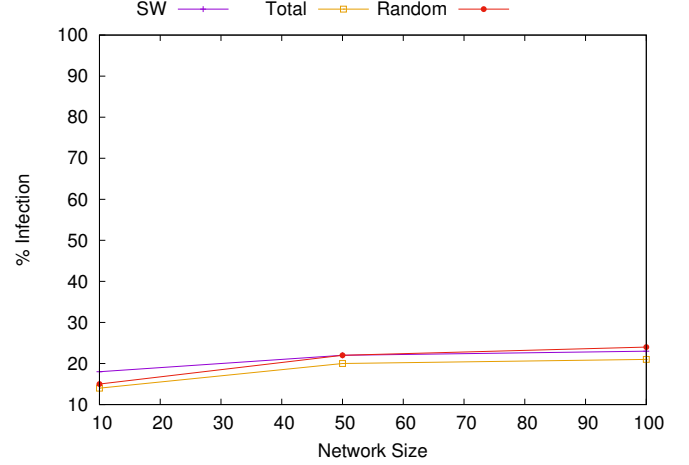Figure 9. Experiment 3: Attack with 10% attackers/discoverers and 0.5 message ranking.

Figure 11. Experiment 5: Attack with 10% attackers/discoverers, 0.5 message ranking and 0.8 network coverage.
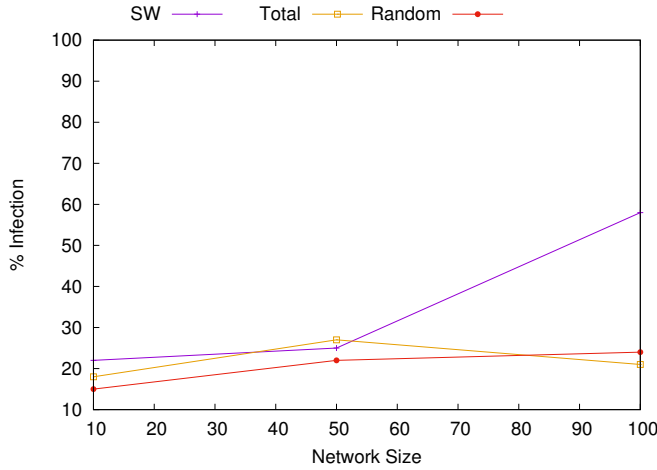

Figure 10. Experiment 4: Attack with 10% attackers/discoverers and 0.8 network coverage.
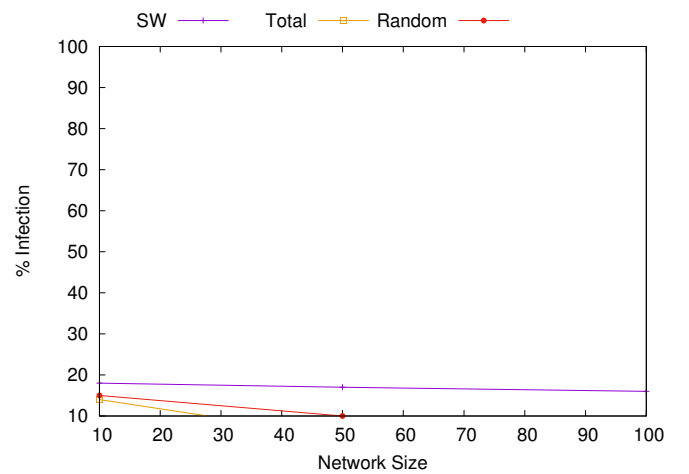

Figure 12. Experiment 6: Attack with 1% attackers, 90% discoverers, 0.5 message ranking and 0.8 network coverage.

from 0.2 to 0.8. There is again a drastic improvement in small newtorks of 10 nodes, and a significant one in larger configurations.

Note that, again, preserving the best results from the first configuration, thus analysing small-world, total and random networks with a single attacker and a proportion of 90% discoverers (i.e. the configuration of Experiment 2 in Figure 8), while rising the level of the variable `network_coverage` from 0.2 to 0.8, no significant improvement in the results is obtained.

5.4. Fourth Configuration: Combined Optimal Parameters

In the last set of experiments, we combine the optimal message ranking and network coverage parameters. We first observe this combination in the non-optimal setting of experiment 1 (Figure 7), i.e. with a proportion of attackers and

of discoverers both fixed at 10% on networks of 10, 50, 100 nodes. The results are plotted in Figure 11, which shows how this configuration manages to keep the infection below 25% in the largest networks and presents an average decrease in infection of over 75% across the three topologies, when compared with the worst-case scenario of experiment 1.

Finally we consider how the optimal configuration of message ranking and network coverages affects the results of Experiment 2 (Figure 8), where the proportion of attackers is minimised to 1% and that of discovered maximised to 90%. Results shown in Figure 12 illustrate how the protocol is able to minimise the negative impact of an attack by a single agent on networks with a large proportion of agents who transmit the truthful data if messaging ranking and network coverage are optimised. The average improvement on the result on the same networks without these last two parameters optimised is of almost 30% across all topologies.

5.5. Summary of Results

The results from the experiments can be summarised as follows:

- the reputation protocol is essential in constraining the attack on networks of any size with at least 10% of the population acting as attackers (an improvement of up to 80% on the same conditions without reputation);
- the protocol is up to 90% more efficient in a one-attacker condition;
- total networks are overall the most efficient topology and in general network size is relevant only when considered in the presence or absence of the reputation protocol.

6. Conclusions

Acknowledgement.

References

[1] *2017 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2017, Paris, France, April 26-28, 2017.* IEEE, 2017.

[2] Brijesh Kumar Chaurasia, Ranjeet Singh Tomar, and Shekhar Verma. Using trust for lightweight communication in vanets. *IJAISC*, 5(2):105–116, 2015.

[3] Nilesh N. Dangare and R. S. Mangrulkar. Design and implementation of trust based approach to mitigate various attacks in mobile ad hoc network. *Procedia Computer Science*, 78(1):554–561, 2016.

[4] Hongmei Deng, Wei Li, and Dharma P. Agrawal. Routing security in wireless ad hoc networks. *Communications Magazine*, pages 70–75, 2002.

[5] John Finnson, Jie Zhang, Thomas T. Tran, Umar Farooq Minhas, and Robin Cohen. A framework for modeling trustworthiness of users in mobile vehicular ad-hoc networks and its validation through simulated traffic flow. In Judith Masthoff, Bamshad Mobasher, Michel C. Desmarais, and Roger Nkambou, editors, *User Modeling, Adaptation, and Personalization - 20th International Conference, UMAP 2012, Montreal, Canada, July 16-20, 2012. Proceedings*, volume 7379 of *Lecture Notes in Computer Science*, pages 76–87. Springer, 2012.

[6] Félix Gómez Mármol and Gregorio Martínez Pérez. Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *J. Netw. Comput. Appl.*, 35(3):934–941, May 2012.

[7] Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, and Muhammad Hanif Durad. Analysis of detection features for wormhole attacks in manets. *Procedia Computer Science*, 56:384 – 390, 2015. The 10th International Conference on Future Networks and Communications (FNC 2015) / The 12th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2015) Affiliated Workshops.

[8] Vinita Jindal and Punam Bedi. Vehicular ad-hoc networks: Introduction, standards, routing protocols and challenges. *IJCSI International Journal of Computer Science Issues*, 13(2):1694–0784, 2016.

[9] Praveen Joshi. Security issues in routing protocols in manets at network layer. *Procedia Computer Science*, 3(1):954–960, 2011.

[10] Nai-Wei Lo and Hsiao-Chien Tsai. A reputation system for traffic safety event on vehicular ad hoc networks. *EURASIP J. Wirel. Commun. Netw.*, 2009:9:1–9:2, April 2009.

[11] U. F. Minhas, Jie Zhang, T. Tran, and R. Cohen. A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. *Trans. Sys. Man Cyber Part C*, 41(3):407–420, May 2011.

[12] Giuseppe Primiero. A calculus for distrust and mistrust. In Sheikh Mahbub Habib, Julita Vassileva, Sjouke Mauw, and Max Mühlhäuser, editors, *Trust Management X - 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings*, volume 473 of *IFIP Advances in Information and Communication Technology*, pages 183–190. Springer, 2016.

[13] Giuseppe Primiero and Franco Raimondi. A typed natural deduction calculus to reason about secure trust. In Ali Miri, Urs Hengartner, Nen-Fu Huang, Audun Jøsang, and Joaquín García-Alfaro, editors, *2014 Twelfth Annual International Conference on Privacy, Security and Trust, Toronto, ON, Canada, July 23-24, 2014*, pages 379–382. IEEE Computer Society, 2014.

[14] Giuseppe Primiero, Franco Raimondi, Taolue Chen, and Rajagopal Nagarajan. A proof-theoretic trust and reputation model for VANET. In *2017 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2017, Paris, France, April 26-28, 2017* [1], pages 146–152.

[15] Maxim Raya, Panagiotis Papadimitratos, Virgil D. Gligor, and Jean-Pierre Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM 2008. 27th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 13-18 April 2008, Phoenix, AZ, USA*, pages 1238–1246. IEEE, 2008.

[16] Arathy K Sa and Sminesh C Na. A novel approach for detection of single and collaborative black hole attacks in manet. *Procedia Computer Science*, pages 264–271, 2016.

[17] Latha Tamilselvan and V. Sankaranarayanan. Prevention of co-operative black hole attack in manet. *Journal of networks 3.5*, pages 13–20, 2008.

[18] Ravi Tomar, Manish Prateek, and G. H. Sastry. Vehicular adhoc network (vanet) - an introduction. *International Journal of Control Theory and Applications*, 9(18):8883–8888, 2016.

[19] R Vanni, L.M.S. Jaimes, G. Mapp, and E. Moreira. Ontology driven reputation model for vanet. In *AICT 2016, The Twelfth Advanced International Conference on Telecommunications, IARIA*, pages 14–19, 2016.

[20] Yu-Chih Wei and Yi-Ming Chen. *Reliability and Efficiency Improvement for Trust Management Model in VANETs*, pages 105–112. Springer Netherlands, Dordrecht, 2012.

[21] Philipp Wex, Jochen Breuer, Albert Held, Tim Leinmüller, and Luca Delgrossi. Trust issues for vehicular ad hoc networks. In *Proceedings of the 67th IEEE Vehicular Technology Conference, VTC Spring 2008, 11-14 May 2008, Singapore*, pages 2800–2804. IEEE, 2008.