An Architecture for Dynamic Trust Monitoring in Mobile Networks

Olufunmilola Onolaja, Rami Bahsoon, and Georgios Theodoropoulos

School of Computer Science,
The University of Birmingham,
United Kingdom,
B15 2TT
{O.O.Onolaja, R.Bahsoon, G.K.Theodoropoulos}@cs.bham.ac.uk

Abstract. Collusion attacks remain a major problem of reputation and trust models, in mobile ad hoc networks. By covering up malicious behaviour of one another from the remaining part of the network, two or more malicious nodes may collaborate to cause damage to or disrupt the network. A number of models exist, which have been proposed to address this issue. Despite these however, the assurance of trusted communication still remains a challenge in these networks. We present a dynamic trust model that detects malicious behaviour at runtime and prevents collusion attacks. Our proposed model employs a novel approach that has the advantage of predicting the future trustworthiness of nodes, based on historical and online behaviour of nodes. This is achieved by an architecture that applies the paradigm of Dynamic Data Driven Application Systems, in solving the problem of collusion attacks in mobile networks.

1 Introduction

In the context of networks, when a node is *trusted*, it implicitly means that the probability that it will perform an action that is beneficial or at least not detrimental in the network is high enough to consider engaging in some form of cooperation with the node [1]. *Reputation* on the other hand, is the opinion of an entity about another; it is the trustworthiness of a node. Both trust and reputation have been used synonymously and adapted to mobile networks.

Behavioural expectation within a mobile network is motivated from the social perspective, where individuals are expected to behave in certain ways within the society. The behaviour of an individual whether good or bad, will determine how others will interact with the individual. The expected behaviour of nodes is to be cooperative in routing and forwarding of packets to neighbouring nodes. *Misbehaviour* among nodes is the deviation from the expected behaviour of nodes in a network. A node is said to be misbehaving once it violates the regular routing and forwarding of packets.

Several Reputation and Trust based Models (RTMs) for mobile networks have been proposed over the years. These models aim to provide information that allows nodes to distinguish between trustworthy and untrustworthy nodes and

R. Meersman, P. Herrero, and T. Dillon (Eds.): OTM 2009 Workshops, LNCS 5872, pp. 494–503, 2009.

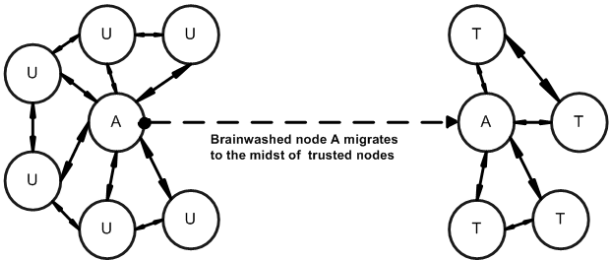

Fig. 1. Brainwashing (U - untrusted, T - trusted)

encourage nodes to be trustworthy. Participation of malicious nodes in network activity is discouraged by existing RTMs. Malicious nodes are isolated, denied service and punished by some of these models.

However, each model addresses some but not all of the problems in mobile networks. Of particular interest is the problem of collusion attacks, where two or more nodes collude to behave maliciously in the network. A scenario of such an attack is *brainwashing*.

Brainwashing; in Fig. 1 describes when colluding and lying nodes surround a node A for example, and the node is tricked into believing false information. When the node moves into a different neighbourhood with trusted and honest nodes, it will not believe them since their information deviates too much from its own. This is a form of collaborative attack because it takes two or more nodes to collude in order to brainwash another.

Without countermeasures, the effects of these attacks have been shown to dramatically affect the security and network performance at runtime [2] as evidenced in poor reliability and quality of service, higher overhead and throughput degradation.

In order to address the problem of collusion attack, we propose a novel approach that uses the Dynamic Data-Driven Application Systems (DDDAS) paradigm [3,4] in ensuring trusted communications in mobile networks. The concepts of the paradigm are applied in building RTMs. This paper aims to show that DDDAS is a potential paradigm for addressing trust related problems in mobile networks.

The remainder of this paper is organised as follows. Sect.2 describes existing research in reputation and trust based models and Sect.3 gives some background on the DDDAS paradigm. Sect.4 and Sect.5 present our contribution and future work respectively. Sect.6 summarises the paper.

2 Related Work

This section summarises the existing work on reputation and trust based models and describes the problems that persist.

A COllaborative REputation mechanism to enforce node cooperation in mobile ad-hoc networks (CORE) [5] model was proposed by Michiardi and Molva.

Reputation in this model is formed and updated with time by direct observations and information provided by other members of the network. Nodes have to contribute continuously to the community to remain trusted or their reputation will be degraded until they are eventually excluded from the network. Only positive information is shared and consequently, CORE prevents the distribution of false information about other entities.

Buchegger *et al.* proposed the Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT) [2] protocol. The protocol aims at detecting and isolating misbehaving nodes, making it unattractive to any node to deny cooperation. In this model, each node maintains a reputation rating and a trust rating about every other node of interest. Only fresh reputation is propagated, with more weight given to current behaviour of a node than the past. This prevents the possibility of a node from obtaining good reputation initially and subsequently misbehaving. Nodes monitor and detect misbehaviour in their neighbourhood by means of an enhanced *packet acknowledgment* (PACK) mechanism where confirmation of acknowledgment comes indirectly by overhearing the next node forward the packet. [6,7]

The Secure and Objective-based Incentive (SORI) scheme aims to encourage packet forwarding, detect and discipline selfishness among network nodes. SORI keeps count of the number of packets requested for forwarding and those actually forwarded by each node. A reputation rating calculated from these counts along with derived confidence and credibility metrics [6,8] is also kept. The propagation of reputation is secured by a one-way hash function, which makes it difficult for a selfish node with a bad reputation to send packets or fake broadcast information, in an attempt to influence its reputation by impersonating a trusted node.

Other more recent work on reputation systems are [9] and others like [10,11] focus on Wireless Sensor Networks (WSNs). The systems aim to distinguish between trustworthy and malicious nodes and to exclude the malicious ones from the network.

A common problem of the models described above is vulnerability to collusion attacks and vulnerability to false praise or accusations. This is because they use a distributed approach to information gathering about node behaviour. That is, each node keeps a record about the behaviour of other nodes of interest. Hence, recommendations provided by individual nodes in the network are used in deciding the reputation of other nodes. While the use of distributed monitoring by these models offers robustness and scalability, there is no repository that collates reputation values. Also, these reputation values are stored and circulated by each node and may lead to collusions and congestion within the network.

These RTMs make use of a component resident on each node called *watchdog* mechanism. This component monitors its neighbourhood and gathers information based on *promiscuous observation.* By promiscuous observation we mean, each node overhears the transmission of neighbouring nodes to detect misbehaviour. Once misbehaviour is detected, the source of the concerned path is notified. This detection mechanism has a weakness of failing to detect a misbehaving node in

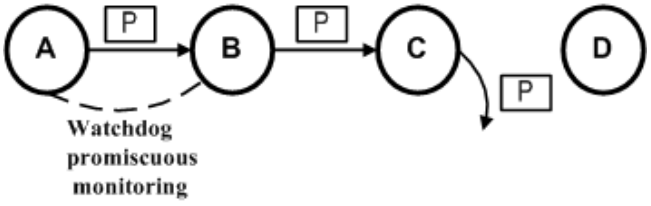

Fig. 2. Node misbehaviour

case of collusions [12]. A form of collusion attack (similar to Fig. 1) that shows the downside of the watchdog mechanism is depicted in Fig. 2.

If node A forwards a packet through B to D. Node C can decide to misbehave and then, collude with B. With the watchdog mechanism, it is possible that B does not report to A when C alters a packet, before forwarding or dropping the packet.

Another problem of the existing models is that they lack a high level of *dynamism* required for such spontaneous networks. They focus mainly on stored Trust Values (TVs) of the nodes with little or no focus on predicting future TVs. We refer to dynamism in terms of the provision of runtime rating by the models and prediction of the future behaviour of each member of the network in order to aid future security-aware decisions in the network. Other problems of these models include:

- The small size of nodes limits their computational power and prevents them from carrying out complex analysis. However, in these models, each node has to maintain reputation information about other nodes;
- Extra computation in accepting observed reputation information;
- The corruption of trust decisions through recommendations made by nodes. These models lack well analysed approaches to determine the bias of each node [9];
- Other security issues such as the modification of data packets by malicious nodes.

To address the problem of collusion attacks, a model with the following is required:

1. Provides dynamic runtime rating of each node based on the cooperation of the nodes;
2. Removes the responsibility of monitoring, calculating and storing of reputation away from the nodes and
3. Predicts the future TVs of nodes by combining historical with the online behaviour of each node.

3 Why Dynamic Data Driven Application Systems (DDDAS)?

The dynamic and volatile nature of Mobile Adhoc Networks (MANETs) makes it difficult to differentiate between normal and malicious network operations. This

therefore, calls for an equally dynamic approach to identifying and isolating misbehaving nodes.

The DDDAS paradigm is a novel approach of symbiotic relation between applications or simulations. In this paradigm, applications can accept and respond dynamically to new data injected into an executing application, and in reverse, such application systems have the ability to dynamically control the measurement processes [4]. The application of the concepts of the paradigm in our model provides dynamism in the detection of malicious nodes and prediction of future behaviour of each node.

In order to address collusion attacks, this research adopts the concepts of the paradigm namely: dynamic *measurement*, *simulation*, *feedback* and *control*. The runtime measurements (behaviour of nodes) are simulated to gain a better understanding and a more accurate prediction of the level of trust for each node. The simulation dynamically measures trust levels, and continually incorporates new measurements at runtime. This will enable the simulation to determine and feedback the reputation of each node into the system. The output of the simulation will help control the network in terms of decisions to be made, to maintain a trusted network. Thus, a trusted third party will be required in the network.

4 Architecture for Dynamic Trust Monitoring

This section introduces our proposed model and discusses how the concepts of DDDAS are adapted in our model. Fig. 3 depicts a conceptual architecture of the model. Table 1 compares the existing models with our proposed model using the functions found in the reputation systems as criteria for comparison.

The [5] model gives a higher weight to past behaviour. The authors argue that a more recent sporadic misbehaviour should have minimal influence on a node's reputation that has been built over a long period of time. In the approach of [2,6] however, the current behaviour of a node carries more weight in order to prevent nodes from obtaining a good reputation and subsequently, misbehaving.

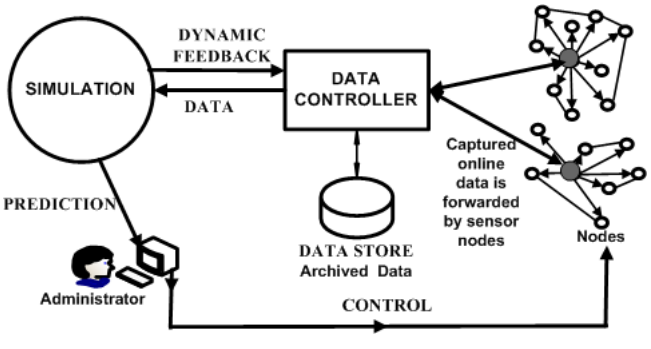

Fig. 3. Conceptual architecture

Table 1. Summary table of reputation and trust models

METRIC	[5]	[2]	[8]	Proposed model
INFORMATION REPRESENTATION	Reputation table with each entry representing a function	Bayesian approach, where ratings are an estimation of the actual probability of misbehaviour	Counters	Reputation table with each entry representing a function
INFORMATION GATHERING	First and second hand information from neighbouring nodes	First and second hand information from neighbouring nodes	First and second hand information from neighbouring nodes	First hand information from SNs
MONITORING	Watchdog	PACK, Watchdog	Watchdog like	Promiscuous monitoring by SNs
TRUST	Not applicable	Adaptive trust	Second hand information/Hash chain based authentication for propagated rating	Authentication of propagated rating
RESPONSE	Isolation	Isolation	Punishment by packet dropping	Isolation
REDEMPTION	Node remains isolated	Periodic reevaluation and reputation fading	No redemption	Periodic reevaluation
DYNAMISM	Ratings are not constant	Periodically updated	Unspecified	Runtime ratings

The later approach will be adopted in our model and runtime *dynamic* change in rating will be incorporated. In our model, online and historical behaviour are considered in determining the runtime reputation of each node and with a higher weight given to recent behaviour.

By comparing the historical behaviour of a mobile node with its online behaviour, misbehaving nodes are detected and excluded. This is because it is assumed that the behaviour of an unauthorised node is different from what is expected. When an untrusted node that violates the expected behaviour is detected through the simulation, adjustments can be made by an administrator or by an automated means. This may result in a *response* such as the exclusion of the node from the network. Also, the result of simulating historical and online behaviour will be used in predicting the expected behaviour of nodes in the future.

Existing reputation based systems lack effective mechanisms for monitoring reputation information, they rely on promiscuous mode of monitoring (an assumption that is not always true in a real mobile ad hoc network); they consequently inherit the watchdog's detection drawback [13]. In the process of capturing information about nodes, these systems introduce additional problems such as collusion attacks. There is therefore a need for an effective approach to *monitoring* the behaviour of nodes, as nodes route and forward packets to adjacent

nodes. We aim to address this need by introducing a monitoring function to the RTM, carried out by Sensor Nodes (SNs).

The use of the SNs is similar to anomaly detection technique in Intrusion Detection Systems (IDSs). The network is partitioned into clusters. Each cluster has a head, which is a SN, and has a direct link with each member of the cluster. The cluster head overhears the traffic to and from all members. Instead of each node operating in a promiscuous mode, the cluster head i.e. the SN in this case, is responsible for *information gathering*. It is assumed that the SNs have a higher capacity in terms of computational power, energy and storage compared to other network nodes. Their function is to monitor nodes in their cluster and are therefore, not susceptible to collusion attacks.

On entrance to the network, a cynical approach is taken, where nodes are not trusted. Each node has a neutral rating until they are able to demonstrate their trustworthiness or maliciousness. The subsequent behaviour of each node will determine an upgrade or downgrade of their TV. Nodes only store TVs of other nodes of interest. If a node needs to forward a packet through a next hop for example, the current reputation of the next hop is sourced from the cluster head.

For each node that misbehaves and is detected, there is a timeout for re-introduction into the network. This process is referred to as *redemption*. This gives a chance for nodes that became faulty for example, to access the network again. If however, the node misbehaves again, it will be isolated at a lower threshold. This is achieved by keeping record of nodes' past behaviour/misbehaviour in the data store shown in Fig. 3.

The components of our proposed model are described in the subsections below:

4.1 Simulation

The incorporation of dynamic inputs (online and archived behaviour) in the simulation, helps with analysis and prediction of the reputation of each node. The output of the simulation provides useful information for the administrator to manage the network or with adequate information to generate an automated response. As described previously, the simulation predicts the future behaviour of nodes by considering their historical behaviour and incorporating their behaviour at runtime.

4.2 Controller

Runtime behaviour of nodes is forwarded to the controller from the SNs. Predictions from the simulation system are fed back to the data controller. This component stores the current reputation value of each node, which may be fetched by the SNs as the need may arise. Reputation is stored in a reputation table with each row containing the reputation score of a particular node. In this architecture, it is assumed that the controller is secure from any form of attacks.

4.3 Sensor Nodes

The role of the SNs is to constantly monitor the behaviour of nodes by acting as cluster head for a group of nodes. They operate in a promiscuous node and overhear transmissions to and from the nodes. SNs gather online information instead of the nodes, because if recommendations made by the nodes are considered; it will give room for collusions and false accusations/praise within the system.

4.4 Data Store

Historical behaviour of nodes are stored and fetched by the controller for simulation from the data store. The *information representation* function is performed by storing the reputation value of each node in a reputation table in this component. It is assumed that nodes have a verifiable identity that is attached to their behaviour. *Trusted* communication will be ensured by the use of a secure one way hash function (similar to [8] discussed in Sect.2) for information transmitted between the intermediate SNs and the nodes that require information about other nodes they wish to communicate with.

In our model, reputation of nodes is not propagated; it is stored on the controller and made available by the intermediary SNs. This is likely to reduce communication overhead considerably. Thus, our proposed approach will

1. Facilitate dynamic changes to ratings of nodes at runtime;
2. Predict the future behaviour of nodes through the simulation of historical data and online behaviour;
3. Detect misbehaving nodes using the simulation system.

Ad hoc networks are traditionally known to lack a central entity. Thus, our model will be most applicable in a semi-ad hoc or WSNs because of the presence of the controller. An example is in high-risk domains that require high security in terms of trust, but need to conserve the mobile nature of the network, such as in military applications.

5 Further Work

We discuss our ongoing research in this section. In the near future, we aim to propose an objective approach for calculating reputation values of nodes. The method with which the simulation system will perform analysis and prediction will be determined. Rigorous tests will be carried out through the simulation of the model and analysis of the results in order to ascertain the effectiveness of our model, in achieving a better overall security.

Ensuring identity persistence is an area that will be explored. This is to prevent excluded or isolated malicious nodes from gaining entrance again into the network, under another identity. Also, the application of our model to the Dynamic Source Routing protocol and its performance will be considered.

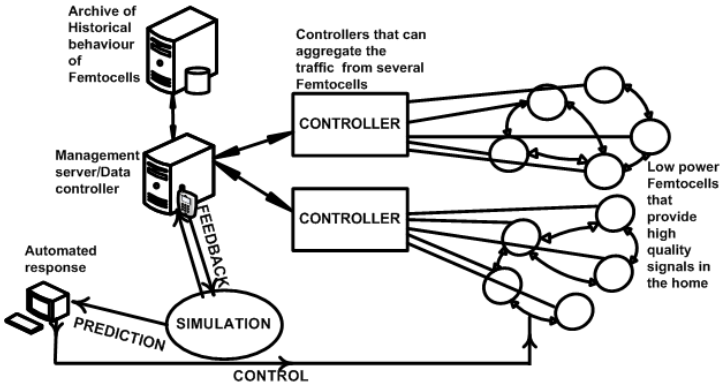

Fig. 4. Instance architecture

We plan to extend this approach to a real life application of the Femtocell technology [14], especially the security issues that arise from the deployment of Femtocells in terms of trusted communication. This technology, which is very new, employs low power cells as cellular access points to connect to a mobile operator's network using residential DSL or cable broadband connections. There has recently been a flurry of activities by mobile phone companies to deploy Femtocells. However, the fact that connection is made via the Internet raises serious security concerns as to how Femtocells can be trusted. Fig. 4 gives an instance architecture showing an application of our model.

6 Conclusion

This paper discusses the pending problems of reputation-based models and how the DDDAS approach can fill the gaps. Our model provides a high level of dynamism to reputation systems by updating the trust values of nodes at runtime. This approach is not only useful at the network level but at a higher level. This will allow for making informed decisions with the dynamic runtime ratings and predictions provided by simulation. We can conclude that the use of runtime monitoring, simulation, feedback and control mechanisms can potentially improve the security of reputation systems.

References

1. Gambetta, D.: Can we trust? Trust: Making and breaking cooperative relations. Basil Blackwell, New York (1988)
2. Buchegger, S., Le Boudec, J.: Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks). In: Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc., pp. 226–236 (2002)

3. Darema, F.: Dynamic data driven applications systems: a new paradigm for application simulations and measurements. In: Bubak, M., van Albada, G.D., Sloot, P.M.A., Dongarra, J. (eds.) ICCS 2004. LNCS, vol. 3038, pp. 662–669. Springer, Heidelberg (2004)
4. Douglas, C.: Dynamic data driven applications systems. In: Bubak, M., van Albada, G.D., Dongarra, J., Sloot, P.M.A. (eds.) ICCS 2008, Part III. LNCS, vol. 5103, pp. 3–4. Springer, Heidelberg (2008)
5. Michiardi, P., Molva, R.: Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Advanced Communications and Multimedia Security, vol. 100, pp. 107–121 (2002)
6. Buchegger, S., Le Boudec, J.: Self-policing mobile ad hoc networks by reputation systems. IEEE Communications Magazine 43(7), 101–107 (2005)
7. Srinivasan, A., Teitelbaum, J., Liang, H., Wu, J., Cardei, M.: Reputation and Trust-based Systems for Ad Hoc and Sensor Networks. In: Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks. Wiley & Sons, Chichester (2006)
8. He, Q., Wu, D., Khosla, P.: Sori: A secure and objective reputation-based incentive scheme for ad-hoc networks. In: Proc. WCNC Wireless Communications and Networking Conference. IEEE Wireless Communications and Networking Conference, vol. 2, pp. 825–830. IEEE, Los Alamitos (2004)
9. Balakrishnan, V., Varadharajan, V., Lucs, P., Tupakula, U.: Trust enhanced secure mobile ad-hoc network routing. In: Advanced Information Networking and Applications Workshops, AINAW 2007, vol. 1, pp. 27–33 (2007)
10. Chen, H., Wu, H., Hu, J., Gao, C.: Event-based trust framework model in wireless sensor networks. In: Proc. International Conference on Networking, Architecture, and Storage, NAS 2008, pp. 359–364 (2008)
11. Ganeriwal, S., Balzano, L.K., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks 4(3), 15:1–37 (2008)
12. Marti, S., Giuli, T., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM, pp. 255–265 (2000)
13. Djenouri, D., Khelladi, L., Badache, A.N.: A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys & Tutorials 7(4), 2–28 (2005)
14. FemtoForum: Femtocell technology (2007), `http://www.femtoforum.org/femto/aboutfemtocells.php`
15. Buchegger, S., Tissieres, C., Le Boudec, J.: A test-bed for misbehavior detection in mobile ad-hoc networks - how much can watchdogs really do? In: Proceedings - IEEE Workshop on Mobile Computing Systems and Applications, WMCSA, pp. 102–111 (2004)
16. Hussain, F., Chang, E., Hussain, O.: State of the art review of the existing bayesian-network based approaches to trust and reputation computation. In: 2nd International Conference on Internet Monitoring and Protection, pp. 154–158 (2007)
17. Rafsanjani, M., Moveghar, A., Koroupi, F.: Investigating intrusion detection systems in manet and comparing idss for detecting misbehaving nodes. In: Proceedings of world academy of Science, Engineering and Technology, pp. 351–355 (2008)