Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 00 (2010) 1–10
Procedia Computer Science

International Conference on Computational Science, ICCS 2010

Conceptual Framework for Dynamic Trust Monitoring and Prediction

Olufunmilola Onolaja*, Rami Bahsoon, Georgios Theodoropoulos

School of Computer Science, The University of Birmingham, United Kingdom, B15 2TT

Abstract

The dynamic and collaborative nature of mobile and sensor networks raises the issue of how connected mobile devices can be trusted. Despite the existing security paradigms such as cryptographic mechanisms, and reputation and trust models, the assurance of security remains a problem of such environments. These networks have been plagued with internal security issues such as the presence of untrusted nodes that misbehave. Depending on the proportion of misbehaving nodes and their strategies, attacks such as collusions may occur. 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. The concept of the Dynamic Data-Driven Application Systems paradigm has been suggested for use in diverse fields. This paper proposes a novel framework that utilises the paradigm in the area of reputation and trust-based systems in mobile networks. The proposed framework is critically evaluated and compared with existing work. This framework, which is applicable to social and behavioural modelling in networks, has the advantage of monitoring and predicting the future trustworthiness of members and highlighting malicious regions within the network.

Keywords: Reputation, Trust, Agent-based modelling, Mobile networks, Collusion

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 one entity about another; it is a measure of 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 a 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 cooperate with the individual. The expected behaviour of nodes in a network for example,

*Corresponding author

Email addresses: O.O.Onolaja@cs.bham.ac.uk (Olufunmilola Onolaja), R.Bahsoon@cs.bham.ac.uk (Rami Bahsoon), G.K.Theodoropoulos@cs.bham.ac.uk (Georgios Theodoropoulos)

is to be cooperative in the routing and forwarding of packets to neighbouring nodes. *Misbehaviour* among nodes is the deviation from the expected behaviour of nodes in a network. Misbehaving nodes are said to be malicious.

Several solutions have been proposed to address the security issues in these networks [2, 3, 4, 5, 6, 7]. Reputation and Trust-based Models (RTMs) are described as systems that provide mechanisms to produce a metric encapsulating reputation for a given domain for each identity within the system [8]. RTMs aim to provide information that allow nodes to distinguish between trustworthy and untrustworthy nodes and encourage nodes to behave as expected. The participation of malicious nodes in network activity is discouraged by the RTMs and malicious nodes are isolated, denied service and punished.

Each model addresses some but not all of the problems or in the process of solving a problem, they introduce other problems. An example is the problem of *collusion attack*, where two or more nodes team up to behave maliciously. Without countermeasures, the effects of this attack have been shown to dramatically affect the security and network performance at runtime as evidenced in poor reliability and quality of service, higher overhead and throughput degradation [3].

The models rely on individual nodes to determine the trust value of the other nodes in the network. More importantly, the prediction of future levels of trustworthiness is not the main focus of the RTMs; they focus mainly on the online reputation and trust of network members. We argue that the existing models lack the level of dynamism required in these networks, which calls for an equally dynamic approach in addressing issues.

The Dynamic Data-Driven Application Systems (DDDAS) [9, 10] paradigm has been applied in diverse fields. Of particular interest are social networks where the utilisation of DDDAS is not extensive [11, 12, 13]. Our research focuses on utilising the paradigm for reputation and trust systems in dynamic and mobile environments.

In an earlier paper [14], we proposed an architecture that aids the elimination of the problem of collusion within a network. This is achieved by a central entity that facilitates the collection of data and provides runtime trust values. In this paper, we extend the central entity to form part of a DDDAS controller that we propose. The idea is that the controller does not only collect the data, but it also predicts future behaviour of nodes. This paper shows how DDDAS is an appropriate paradigm for predicting trust related problems in mobile and sensor networks. Our contribution is a framework capable of providing dynamic changes to trust ratings of nodes at runtime and predicting the future behaviour of nodes through the simulation of historical data and online behaviour.

The remainder of this paper is organised as follows: Section 2 describes existing reputation and trust-based models and the existing problems. The motivation for the use of the DDDAS paradigm in this research is discussed in Section 3. The proposed framework for reputation systems is described in the following section. Section 5 details the challenges and the future direction of this research and the last section summarises the paper.

2. Reputation and Trust-based Models

A suggested approach for addressing security issues in mobile and sensor networks is the use of public key and identity-based cryptography. These mechanisms, though effective, are not very suitable due to the limitation of node resources. Cryptographic solutions are limited by the fact that adversaries can gain access to valid keys by physically compromising a node. Compromised nodes can then insert bogus data into the network [4]. Despite the fact that researchers have come up with less computational intensive cryptographic mechanisms, several limitations remain. These include high mobility, limited memory, the processing and battery power of nodes to mention a few [15, 16, 17, 18].

Due to the inadequacy of cryptographic mechanisms, researchers proposed RTMs, which have shown positive results. Michiardi and Molva [2] proposed a model where reputation 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 else, their reputation will be degraded until they are eventually excluded from the network. The 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.

Buchegger *et al.* [3] proposed a protocol that aims to detect and isolate misbehaving nodes, making it unattractive for any node to deny cooperation with others. In this framework, each node maintains a reputation rating and a trust rating about every other node of interest. Only fresh reputation is propagated in the network, with more weight given to the current behaviour of a node over its past behaviour. Nodes monitor and detect misbehaviour in their

neighbourhood by means of an enhanced *packet acknowledgment* (PACK) mechanism; where the confirmation of acknowledgment comes indirectly by overhearing the next node forward the packet [19, 20].

In the work of Ganeriwal *et al.* [4], which is applicable to wireless sensor networks, each sensor node maintains reputation metrics. These metrics represent the past behaviour of other nodes and are used as an inherent aspect in predicting their future behaviour. The model relies on network members to maintain the reputation of others based on their experiences and uses this to evaluate their trustworthiness.

The more recent studies on reputation systems are discussed in [5, 6, 7]. A common problem of some of the models includes vulnerability to collusion attacks and vulnerability to false praise or accusations [21]. The problem is as a result of the use of a distributed approach to information gathering about node behaviour. That is, each node keeps a record about the behaviour of other nodes of interest. The recommendations provided by individual nodes in the network are used in deciding the reputation of other nodes. Also, reputation information is stored and circulated by each node, which may lead to collusions and network congestion. While the distributed approach offers robustness and scalability, there is no repository that collates reputation information.

The RTMs make use of a component resident on each node called *watchdog* mechanism. This component monitors its neighbourhood and gathers data by *promiscuous observation*. By promiscuous observation we mean that each node overhears the transmission of neighbouring nodes to detect misbehaviour. If the watchdog notices the neighbour's transmission matches the expected template transmission, a positive reputation value is stored in the appropriate table. Once misbehaviour is detected, a negative reputation value is stored. This detection mechanism has a weakness of failing to detect a misbehaving node in case of collusions [22]. Figure 1 depicts a form of collusion attack showing the downside of the watchdog mechanism.

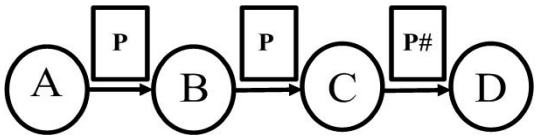

Figure 1. Node misbehaviour

In a normal situation, node *A* forwards the packet to node *B* and *B* forwards the packet to node *C*. Node *C* then forwards the packet to node *D*. However, node *C* may decide to alter the packet before sending it to *D*. Furthermore, node *B* colludes with *C* by refusing to notify *A* of node *C*'s action. With the watchdog mechanism, it is possible that *B* does not report to *A* when *C* alters a packet *P* to *P#*, before forwarding or dropping the packet. Malicious nodes in promiscuous mode do not only have the chance to collude but can also capture sensitive data such as passwords and personal identification numbers being exchanged.

Let us consider a similar attack where two nodes *A* and *B* are controlled by an attacker. If *A* tells *B* all of its secrets, then *B* can masquerade as *A* to all of *B*'s neighbours that node *A* shares pair wise keys with and vice versa. The keys from each subsequently obtained node, can be reused by the other attacker controlled nodes, cascading the impact of the compromise. Therefore, an attacker can control a node undetectably by physically compromising the node, and the node in turn compromising other nodes within the network [23].

Another problem of the existing models is that they lack a high level of *dynamism* required for such spontaneous networks. We refer to dynamism in terms of the provision of runtime ratings by the models and prediction of the future behaviour of each member of the network. These models focus mainly on current Trust Values (TVs) of the nodes, with little or no focus on predicting future TVs.

The small size of network nodes limits their computational power, preventing them from carrying out the complex analysis required by some models. Extra computation in accepting observed reputation information from other nodes remains a problem. Also, these models lack well-analysed approaches to determine the bias of each node [5]. Trust decisions can be corrupted through recommendations made by nodes and malicious nodes can modify data packets, as shown in Figure 1.

3. Why Dynamic Data-Driven Application Systems?

The dynamic and volatile nature of mobile and sensor networks make it difficult to differentiate between normal and malicious network behaviour. This nature therefore, calls for an equally dynamic approach to identifying and isolating misbehaving nodes. In traditional reputation systems, there are some missing elements that are listed below:

i. Provision of dynamic TVs of network members to identify malicious nodes at runtime,
ii. Prediction of future TVs of nodes to prevent nodes from misbehaving and
iii. Network organisation into regions of risk to focus on regions of high risk.

To fill the missing gaps, a framework with the following characteristics is required:

i. Provides dynamic runtime rating of nodes using data provided from the network,
ii. Prevents nodes' bias from influencing trust decisions and
iii. Predicts the future TVs by analysing the behaviour of individual nodes over time.

Current research in DDDAS focus on simulation of physical, artificial or social entities. The simulation is able to make predictions about how the entity would evolve and its future state. The predictions made by the simulation can then influence how and where future data will be gathered from the entity, in order to focus on areas of uncertainty [11].

Hence, the DDDAS paradigm is that of a symbiotic relationship between reality and simulations. The application of the paradigm's concept in this framework provides dynamism in the detection of malicious nodes and prediction of future behaviour. The runtime behaviour (data) of nodes is simulated to gain a better understanding and a more accurate prediction of the level of trust for each node. This predictive capability is similar to the model suggested in [4]. Here, each sensor node maintains reputation metrics, which represent the past behaviour of other nodes. The reputation metrics are used to predict future behaviour of nodes.

By employing DDDAS, the simulation is capable of dynamically measuring trust levels, and continually incorporating new data at runtime. The output from the simulation will help control the network in terms of decisions to be made in order to maintain a trusted network.

4. Framework for dynamic trust monitoring and prediction

This section introduces the framework and gives a comparative analysis with pre-existing ones. Figure 2 depicts a conceptual architecture of the framework and Table 1 compares the existing models with our proposed model using the criteria described in this section.

At initialisation, each node is assigned a neutral TV until they are able to demonstrate their trustworthiness or maliciousness. The observed behaviour of each node will determine the adjustment of their TVs accordingly. In the framework, useful data is selected from a stream of data from the network and is dynamically injected into the *controller* to determine the current TVs of network members. The *simulation* of the entire network utilises the processed data to predict the future behaviour of members. The final aim of the system is to group nodes into different regions of trust depending on their level of trust. This enables decision makers and other stakeholders to focus on regions of high risk.

Considering the calculation of TVs, the model described by [2] 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, which has been built over a long period of time. In contrast, in the approach of [3, 19], the current behaviour of a node carries more weight to prevent nodes from obtaining a good reputation and subsequently, misbehaving. The latter approach is adopted in this research, with a higher weight given to recent behaviour. This is described further in Section 4.2.

By comparing the historical behaviour of a node with its online behaviour, runtime dynamic change in rating is incorporated in trust ratings and misbehaving nodes are detected. This is based on the assumption that the behaviour of a malicious node is different from its expected behaviour. Using as an example, a scenario of criminal monitoring with each suspect having a mobile phone, the expectation is that the phone is used within a certain geographical radius. When an untrusted individual that violates the expected behaviour (using techniques such as text mining or voice recognition) is detected by the controller, adjustments can be made such as a *response* of exclusion from the rest of the network.

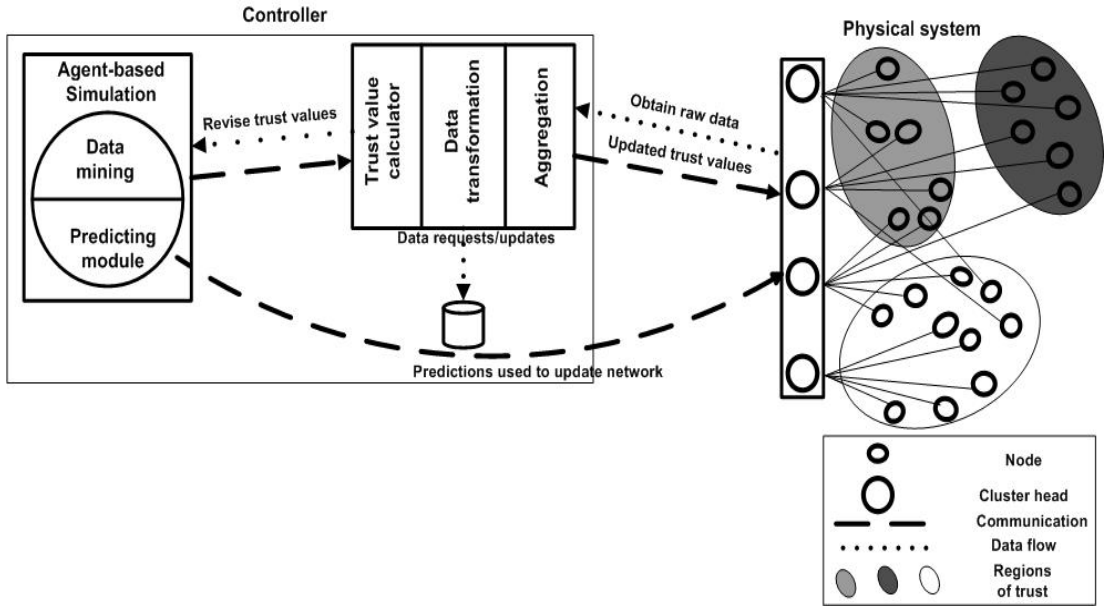

Figure 2. High-level diagram showing the components of the proposed framework

As discussed in Section 2, reputation-based systems lack effective mechanisms for monitoring reputation information. They rely on the promiscuous mode of monitoring (an assumption that is not always true in a real network). Consequently, they inherit the watchdog's detection weakness [24]. In the process of capturing information about nodes, these systems introduce additional problems such as collusion attacks. Therefore, there is a need for an effective approach to *monitoring* the behaviour of nodes. This is addressed in the proposed framework with the introduction of a monitoring function by Cluster Heads (CHs). The network is physically partitioned into clusters and each cluster has a head. Upon entering the network, each node registers its presence with a CH. Each CH has a direct link with all members of its cluster and overhears all the communication between the members. The CH is responsible for *information gathering*; that is, the collection of data. This therefore does not require member nodes to operate in promiscuous mode. It is assumed that the CHs have a higher capacity in terms of computational power, energy, and storage compared to other network nodes. The function of CHs is to monitor the nodes in their cluster; they are therefore not susceptible to collusion attacks.

The information that is gathered from the simulation help to identify regions of high-risk, medium-risk and low-risk in the network. Nodes are then assigned to the different regions, depending on their reputation (as depicted in Figure 2). The grouping helps in the management of the network by focusing on critical group of nodes that require more attention. This will equally aid future security-aware decisions in the network.

The components of our proposed model are described below:

4.1. Physical system

In the framework (see Figure 2), the physical system comprises of nodes in a network exchanging information or collaborating with each other. Nodes may, for example, be in the form of mobile phones, payment cards or other tokens with a unique identity. Each node belongs to a region of trust which may either be of high-risk, medium-risk or low-risk as shown in Table 2.

The reputation of a node is the collection of ratings maintained by the controller about this node. The reputation of a given region is determined by the collective ratings of the member nodes. The regions of trust will depend on how the network evolves over time and the idea of clustering (described earlier) is a physical structure of the network.

The role of the CH is to constantly monitor the behaviour of nodes and to act as an online data source in the network. The CHs are responsible for gathering online data instead of the nodes; the CHs perform this function by operating in a promiscuous mode, enabling them to overhear all transmissions between nodes. This approach is

Table 1. Summary table comparing existing reputation and trust models with proposed framework

Criteria / Model	[2]	[3]	[4]	Framework
Information Representation	Heuristic approach using a reputation table with each entry representing a function	Bayesian approach, where ratings are an estimation of the actual probability of misbehaviour	Bayesian formulation based on decision theory	Trust formulation with each node having a probabilistic discrete value
Information Gathering	First and second hand information from neighbouring nodes	First and second hand information from neighbouring nodes	Integration of direct and second hand observations	Observations in the form of data from sensors to the controller
Monitoring	Watchdog mechanism	Packet acknowledgment, Watchdog mechanism	Watchdog mechanism	Monitoring of directly connected nodes by cluster heads
Simulation	Not applicable	Not applicable	Not applicable	Simulation of physical network
Response	Isolation	Isolation	Exclusion (avoidance)	Domain dependent
Dynamism	Ratings are not constant	Periodically updated	Provides real time feedback	Runtime ratings and feedback
Prediction	Not applicable	Not applicable	Trust metric that is representative of a nodes' future behaviour	Prediction of trust values by simulation, where values are a probability of misbehaviour

adopted because recommendations made by the individual nodes give room for collusions and other attacks such as, false accusations and praises.

4.2. Controller

The data controller works with the CHs to obtain and filter data. It is assumed that the controller is secure from any form of attack. Depending on the domain of application, it is possible to have back-up controllers in order to avoid a single point of failure and to provide redundancy within the framework.

The approach adopted in this framework is such that runtime data about node behaviour is forwarded to the controller. The data is then transformed into a corresponding value, which is used to calculate the online TV of each node. The controller includes an *Aggregator*, a *Data Transformer*, a *Trust Value Calculator*, a *Data Repository* and the *Simulation*, described below:

- Aggregator: Data, which is a representation of the behaviour and collaboration among nodes, is collected from the data sources. The requirement for data to be admitted into the controller is to meet the specified criteria. The criteria help in identifying relevant data such as data about nodes with a low TV, or nodes in the high-risk region and simply discard irrelevant data. Using the scenario of a criminal-monitoring network for example, the collaboration of an individual with a suspect is flagged as important data to be added. The collected data reflects the current state of the network at a specific point in time.

- Data transformer: In order for a reputation system to function as it ought to, observations and experiences have to be captured and represented numerically. That is, the qualitative data captured need to converted to a quantitative data. Therefore, node behaviour is captured, quantified and measured by an associated TV.

Table 2. Trust table showing the degrees of trust and corresponding regions of risk

Trust Value	Meaning	Description	Region
5	Complete trust	Trusted node with an excellent reputation	Low risk
4	Good trust level	Very reliable node	Low risk
3	Average trust level	Average value and somewhat reliable node	Medium risk
2	Average trust level	Average value but questionable node	Medium risk
1	Poor trust level	A questionable node	High risk
0	Complete distrust	Malicious node with a bad reputation	High risk

Every behavioural expectation in the network has a corresponding value and the collection of these values will eventually determine a node's online TV. The act of collaborating with a suspected malicious individual, with a predefined value of `1` for example, will result in a downgrade of the TV of a trusted node.

A set of discrete trust values is assumed in the framework and each value represents a degree of trust as described in Table 2. These discrete degrees of trust introduce flexibility into the application of our framework, because different behaviours correspond to different levels of trust. Data that has been collected from the network is then transformed into a form that can be used to determine the tv of each node. The data is converted to a value ranging from [0, 5], where a score of 0 means a node is completely untrusted, 5 means a node is absolutely trusted and if $0 < \mathtt{TV} < 5$, then it implies that the node is trusted to a certain extent.

- Trust value calculator: Computing trust in RTMs has been described as an abstract mathematical specification of how available information should be transformed into a usable metric [8]. In this framework, the specification is made through explicit equations, discussed below in this section. Trust computation is very difficult, as trust has to be defined in a very precise way because the computation of trust is crucial to the fulfilment of the functions of any trust-based framework.

  Nodes are expected to act in certain ways and the expected behaviour is domain dependent. We model the expected behaviour in the framework with predefined values and any contrary action in the domain is flagged as a possible malicious attack and a downgrade of the trust rating of the node.

  The TV's of network members are dynamically updated at specified time intervals `j` in our framework, where $\mathtt{j} = \{1, 2, \ldots, \mathtt{i\text{-}1}\}$. Note that `i` represents the current time while `i-1` is the last time a snapshot of the physical system was taken. Using the notation of $\mathtt{tv_h}$ to represent the historical TV, we define the trust value $\mathtt{tv_h}$ of a node with time to be

$$\mathtt{tv}_{\mathtt{h}}^{(i)} = \frac{1}{\mathtt{i\text{-}1}} \sum_{j=1}^{i-1} (\mathtt{tv_n})^{(j)} \tag{1}$$

  That is,

$$\mathtt{tv}_{\mathtt{h}}^{(i)} = \frac{(\mathtt{tv_n})^{(1)} + (\mathtt{tv_n})^{(2)} + (\mathtt{tv_n})^{(3)} + \ldots + (\mathtt{tv_n})^{(i-1)}}{\mathtt{i\text{-}1}} \tag{2}$$

  which is the average of the sum of the previous TVs up until the time `i-1`. We denote the online TV, derived from nodes' recent activity as $\mathtt{tv_o}$. This is the sum of observations captured and represented numerically for

each node. The new TV $\mathtt{tv_n}$ of a node at time $\mathtt{i}$ is defined as

$$\mathtt{tv}_{\mathtt{n}}^{(i)} = \frac{((\mu_{\mathtt{h}}\mathtt{tv_h}) + (\mu_{\mathtt{o}}\mathtt{tv_o}))^{(i)}}{\mu_{\mathtt{h}}\mu_{\mathtt{o}}} \tag{3}$$

Weights $\mu_{\mathtt{o}}$ and $\mu_{\mathtt{h}}$ (factors for the online and historical TVs respectively) are introduced to control the effect of historical behaviour of nodes on their new TVs. In the framework, $[\mu_{\mathtt{o}}, \mu_{\mathtt{h}}] > 0$ and $\mu_{\mathtt{o}} > \mu_{\mathtt{h}}$, thereby placing more emphasis on recent behaviour. For example, let us consider a node with an average historical value of 3 and online value of 4, if $\mu_{\mathtt{h}} = 2$ and $\mu_{\mathtt{o}} = 3$, we obtain $\mathtt{tv_n} = 3$. The emphasis on online behaviour prevents nodes from gaining trust by behaving as expected over a sustained period of time and only then start to misbehave; referred to as an *intoxication attack* [19, 25]. This attack occurs because the effect of historical good behaviour outweighs the effect of current actions on reputation.

- Data repository: Within this framework, it is assumed that nodes have a verifiable and persistent identity attached to their behaviour. The repository acts as a historical data source and archive. The *information representation* function is performed by storing the trust value of every network member on a reputation table, with each row of the table containing the TVs of a uniquely identifiable node. Historical behaviour of nodes are stored as TVs and fetched from the data repository to be used as evidence in order to predict future possible values.

- Simulation: The aim of the simulation is to identify regions of high-risk, medium-risk and low-risk as described earlier. Although the physical network is divided into clusters, nodes are assigned to regions based on their level of risk to the network. The level of risk the node poses is determined by the probability of the nodes' misbehaviour and considering the reputation ($\mathtt{tv_h}$) of the node.

  Dynamic data (online behaviour) are incorporated in the simulation, which helps with the analysis and prediction of node reputation. We are interested in modelling the application level behaviour of each node in the system rather than the low level protocols involved in the network. To this end, the proposed framework utilises an agent-based simulation: Repast[1] to implement its predictive capabilities. Based on the behavioural rules incorporated into the nodes in the simulation, the predicted TVs of each node change using probabilities of collaboration among the nodes. These changes are indicators of the possible expectations in the physical system.

  If there are any discrepancies between the predicted value and the TVs in reality, questions are raised and the role of the simulation is to find answers to the questions. Assuming a node *A* (in a low-risk region) collaborates with a node *B* (in a high-risk region), what happens to the TV of node *A*? Will *A* be moved to a high-risk region? What could make *A* and *B* collude? How will the regions evolve over time? These scenarios are considered using the agent-based simulation.

  The simulation considers the probability of a node misbehaving and the probability of collaboration between the two or more nodes. This is done using the predefined behavioural rules incorporated in the nodes in simulation. The simulation system uses a continuous learning process that uses knowledge converted from captured evidence to predict future possible behaviour of nodes. This component improves the predictive capability of the framework and provides adequate feedback that enables for example, the administrator to manage and control the network by making security-aware decisions.

5. Future work and discussion

Ad hoc networks are traditionally known to lack a central entity; therefore, this framework will be most applicable in semi-ad hoc or sensor network environments that lend themselves to centralised control. An example is in high-risk domains such as the military and in criminal monitoring, which require high-level of security in terms of trust and central control, but need to conserve the mobile nature of the network.

[1] http://repast.sourceforge.net/

Data mining for discovering patterns in data obtained is a challenge in this research because valid patterns of node behaviour have to be detected as data is collected. The interpretation of the data and the translation to trust values is important to the success of this work. An appropriate prediction technique, which ensures that accurate predictions are made, serves as a direction of future work. The dynamic and mission critical nature of the applicable domains set strict time constraints in communication. For instance, the detection of criminal behaviour should be immediately communicated to the police.

The proposed system is currently being implemented, using Repast as a simulation toolkit. Once complete, we anticipate the use of the system in real-life applications such as criminal monitoring. As a first case study, we envision a scenario of tracing suspects (nodes) by their phone usage (behaviour) with the provider substations acting as CHs. Rigorous tests will be carried out through the simulation of the model and analysis of the results in order to ascertain the effectiveness of this framework, in achieving a better overall security.

6. Conclusion

This paper proposes a dynamic reputation and trust-based framework that is able to predict the behaviour of network members in the future. Our framework provides a high level of dynamism to reputation systems by updating the trust values of nodes at runtime. In addition, the framework is useful for grouping network members into different regions of trust in order to focus on regions of high-risk. The proposed approach is not only useful at the network level but at a higher level, providing adequate information that allows for countermeasures and making security aware decisions in the network by stakeholders. It can therefore be concluded that the use of runtime monitoring and measurement, simulation of the physical system, feedback in terms of prediction and control mechanisms, can potentially improve the security in reputation and trust systems.

References

[1] D. Gambetta, Can we trust?, Trust: Making and Breaking Cooperative Relations Edition, Basil Blackwell, New York, 1988.
[2] P. Michiardi, 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, Vol. 100, Kluwer, B.V., 2002, pp. 107–121.
[3] S. Buchegger, J. Le Boudec, 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, 2002, pp. 226–236.
[4] S. Ganeriwal, L. K. Balzano, M. B. Srivastava, Reputation-based framework for high integrity sensor networks, ACM Transactions on Sensor Networks 4 (3) (2008) 15:1–37.
[5] V. Balakrishnan, V. Varadharajan, P. Lucs, U. Tupakula, Trust enhanced secure mobile ad-hoc network routing, in: Advanced Information Networking and Applications Workshops, AINAW'07, Vol. 1, 2007, pp. 27–33.
[6] Q. He, D. Wu, P. Khosla, SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks, in: Proceedings of WCNC Wireless Communications and Networking Conference, Vol. 2 of IEEE Wireless Communications and Networking Conference, 2004, pp. 825–830.
[7] H. Chen, H. Wu, J. Hu, C. Gao, Event-based trust framework model in wireless sensor networks, in: NAS '08: Proceedings of the 2008 International Conference on Networking, Architecture, and Storage, IEEE Computer Society, 2008, pp. 359–364.
[8] K. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Computing Surveys 42 (1) (2009) 1–31.
[9] F. Darema, Dynamic Data Driven Applications Systems: A New Paradigm for Application Simulations and Measurements, in: International Conference on Computational Science, 2004, pp. 662–669.
[10] C. Douglas, Dynamic Data Driven Applications Systems, in: International Conference on Computational Science ICCS (3), Vol. 5103 LNCS, 2008, pp. 3–4.
[11] C. Kennedy, G. Theodoropoulos, Intelligent management of data driven simulations to support model building in the social sciences, Computational Science-ICCS 2006. 6th International Conference. Proceedings, Part III (Lecture Notes in Computer Science) 3993 (2006) 562 – 569.
[12] C. Kennedy, G. Theodoropoulos, V. Sorge, E. Ferrari, P. Lee, C. Skelcher, AIMSS: An architecture for data driven simulations in the social sciences, in: Lecture Notes in Computer Science, Vol. 4487 LNCS, 2007, pp. 1098 – 1105.
[13] G. Madey, G. Szabo, A. Barabasi, WIPER: the integrated wireless phone based emergency response system, in: Computational Science-ICCS 2006. 6th International Conference. Proceedings, Part III (Lecture Notes in Computer Science Vol.3993), Vol. 3993 LNCS, 2006, pp. 417 – 424.
[14] O. Onolaja, R. Bahsoon, G. Theodoropoulos, An Architecture for Dynamic Trust Monitoring in Mobile Networks, in: Lecture Notes in Computer Science, Vol. 5872 LNCS, 2009, pp. 494 – 503.
[15] L. Eschenauer, V. D. Gligor, A key-management scheme for distributed sensor networks, in: CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, ACM, 2002, pp. 41 – 47.

[16] Y. Fang, X. Zhu, Y. Zhang, Securing resource-constrained wireless ad hoc networks, IEEE Wireless Communications 16 (2) (2009) 24 – 30.
[17] D. Liu, P. Ning, L. Rongfang, Establishing pairwise keys in distributed sensor networks, ACM Transactions on Information and System Security 8 (1) (2005) 41 – 77.
[18] C. Zhang, M. Zhou, M. Yu, Ad hoc network routing and security: A review, International Journal of Communication Systems 20 (8) (2007) 909 – 925.
[19] S. Buchegger, J. Le Boudec, Self-policing mobile ad hoc networks by reputation systems, IEEE Communications Magazine 43 (7) (2005) 101–107.
[20] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, M. Cardei, Reputation and Trust-based Systems for Ad Hoc and Sensor Networks, In Algorithms and Protocols for Wireless Ad Hoc Networks, Wiley & Sons, 2008.
[21] J. Hu, M. Burmester, LARS - A locally aware reputation system for mobile ad hoc networks, in: Proceedings of the ACM SE Regional Conference, Vol. 2006, 2006, pp. 119 – 123.
[22] S. Marti, T. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM, 2000, pp. 255–265.
[23] T. Moore, A collusion attack on pairwise key predistribution schemes for distributed sensor networks, in: Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops, Vol. 2006, 2006, pp. 251 – 255.
[24] D. Djenouri, L. Khelladi, A. N. Badache, A survey of security issues in mobile ad hoc and sensor networks, Communications Surveys & Tutorials, IEEE 7 (4) (2005) 2–28.
[25] M. Azer, S. El-Kassas, A. Hassan, M. El-Soudani, A survey on trust and reputation schemes in ad hoc networks, in: ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, IEEE Computer Society, 2008, pp. 881 – 886.