# Reputation and Trust-based Systems for Ad Hoc and Sensor Networks

Avinash Srinivasan†, Joshua Teitelbaum†, Huigang Liang‡,
Jie Wu†and Mihaela Cardei†
†Department of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL 33431
Email: {asriniva@, jteitel2@, jie@cse., mihaela@cse.}fau.edu
‡Department of ITOM
College of Business
Florida Atlantic University
Ft. Lauderdale, FL 33301
Email: hliang@fau.edu

## 1 Introduction

Reputation and trust are two very useful tools that are used to facilitate decision making in diverse fields from an ancient fish market to state-of-the-art e-commerce. Reputation is the opinion of one entity about another. In an absolute context, it is the trustworthiness of an entity [26]. Trust, on the other hand, is the expectation of one entity about the actions of another [23]. For over three decades, formal studies have been done on how reputation and trust can affect decision making abilities in uncertain conditions. Only recently has trust and reputation been adapted to wireless communication networks. Trust is a multi-dimensional entity which, if effectively modeled, can resolve many problems in wireless communication networks.

Wireless communication networks, mobile ad-hoc networks (MANETs) and wireless sensor networks (WSNs) in particular, have undergone tremendous technological advances over the last few years. With this development comes the

risk of newer threats and challenges, along with the responsibility of ensuring the safety, security, and integrity of information communication over these networks. MANETs, due to the individualized nature of the member nodes, are particularly vulnerable to selfish behavior. Because each node labors under a energy constraint, there is incentive for a node to be programmed to selfishly guard its resource, leading it to behave in a manner that is harmful to the network as a whole.

WSNs, on the other hand, are open to unique problems due to their usual operation in unattended and hostile areas. Since sensor networks are deployed with thousands of sensors to monitor even a small area, it becomes imperative to produce sensors at very low costs. This inevitably dilutes the tamper resistant property of sensors. The aforementioned unique situation of WSNs leaves the nodes in the network open to physical capture by an adversary. Because each node has valid cryptographic key information, standard cryptographic security can be bypassed. The adversary has as much knowledge about the system as was available to the node itself, and is therefor able to reprogram the captured node in such a way as to cause maximum damage to the system.

These problems can be resolved by modeling MANETs and WSNs as reputation and trust-based systems. As in real life, we tend to believe and interact only with people who we see as having a good reputation. Reputation can be defined as a person's history of behavior, and can be positive, negative, or a mix of both. Based on this reputation, trust is built. Trust can be seen as the expectation that a person will act in a certain way. For example, if a person has a reputation for not getting jobs done, then people will not trust that this person will get a job done in the future. Based on this, people will not assign critical jobs to him, since they believe there is a good chance that he will not get the job done.

Similarly, nodes in MANETs and WSNs can make reputation and trust guided decisions, for example in choosing relay nodes for forwarding packets for other nodes, or for accepting location information from beacon nodes as in [26]. This not only provides MANETs and WSNs with the capability of informed decision making, but also provides them security in the face of internal attacks where cryptographic security gives way. The way in which a system discovers, records, and utilizes reputation to form trust, and uses trust to influence behavior is referred to as a reputation and trust-based system. This chapter is dedicated to providing the reader with a complete understanding of reputation and trust-based systems from the wireless communication perspective.

The rest of this chapter is organized as follows. In Section 2, we will give an in depth background of reputation and trust from social perspective. Then in Sec-

tion 3, we will present reputation and trust from network perspective and discuss various challenges in modeling networks as reputation and trust-based systems. We move on to present the reputation and trust-based systems discussing their goals, properties, initialization, and classification in Section 4. Then in Section 5, we will discuss the components of reputation and trust-based systems in detail. In Section 6 we will present the current reputation and trust-based systems that are in use. We have presented the current open problems in reputation and trust-based systems from the network perspective in Section 7. Finally in Section 8 we conclude this chapter.

# 2 Social Perspective

In this section we provide an in depth discussion on trust and uncertainty from a societal perspective and use e-commerce in the cyber space to illustrate various concepts. Trust and uncertainty have played a very critical role in the market place, modeling both consumer and seller behavior and providing a great deal of insight into meaningful transactions. We first define trust and uncertainty in a general framework exploring their causal-effect relationship. Then we discuss the various trust antecedents. Finally, we end the section with a brief discussion on information asymmetry and opportunistic behavior.

## 2.1 Trust and Uncertainty

Trust has been widely recognized as an important factor affecting consumer behavior, especially in the e-commerce context where uncertainty abounds. Trust is necessary only when there is uncertainty. Transaction economics research demonstrates that uncertainty increases transaction cost and decreases acceptance of online shopping [30]. The Internet environment is uncertain and consumers' perceived uncertainty deters their adoption of online shopping [31]. Trust contributes to e-commerce success by helping consumers overcome uncertainty.

Trust is complex and multidimensional in nature. Multiple research streams in the past have shed light on various antecedents of trust. Major antecedents of trust include calculus-based trust, knowledge-based trust, and institution-based trust [27, 28, 29].

Uncertainty originates from two sources: *information asymmetry* and *opportunism*. The former refers to the fact that either party may not have access to all of the information it needs. The latter indicates that different goals exist between

transacting partners and both parties tend to behave opportunistically to serve their self-interests.

## 2.2 Trust Beliefs and Trust Intention

Trust means that the trustor believes in, and is willing to depend on, the trustee [28]. Based on the theory of reasoned action, McKnight et al. [36] breaks the high level trust concept into two constructs, trusting beliefs and trusting intention. Trusting beliefs are multidimensional, representing one's beliefs that the trustee is likely to behave in a way that is benevolent, competent, honest, or predictable in a situation. According to McKnight et al. [27], three trusting beliefs appeared most frequently in trust research: *competence*, *benevolence*, and *integrity*. Trusting intention is the extent to which one is willing to depend on the other person in a given situation. Stewart [32] explained that there are several intended actions that represent trusting intentions such as the intent to continue a relationship, the intent to pursue long term orientation toward future goals, and the intent to make a purchase. Theory of reasoned action supports the proposition that "positive beliefs regarding an action have a positive effect on intentions to perform that action" [32]. Trusting beliefs have been found to have a significant positive influence on trusting intention [27].

Trust is a critical aspect of e-commerce. Online purchase renders a customer vulnerable in many ways due to the lack of proven guarantees that an e-vendor will not behave opportunistically. The Internet is a complex social environment, which still lacks effective regulation. When a social environment cannot be regulated through rules and customs, people adopt trust as a central social complexity reduction strategy. Therefore, online customers have to trust an e-vendor from which they purchase; otherwise, the social complexity will cause them to avoid purchasing [29].

## 2.3 Calculus-based Trust Antecedents

In economic transactions, parties develop trust in a calculative manner [33]. To make a calculus-based trust choice, one party rationally calculates the costs and benefits of other party's cheating or cooperating in the transaction. Trust develops if the probability of that party performing an action that is beneficial or at least not detrimental to the first party is high [33].

Consumers can obtain pieces of information regarding an e-vendor's trustworthiness through a variety of channels. Calculus-based trust develops because

of credible information regarding the intentions or competence of the trustee. The credible information, such as reputation and certification, can signal that the trustee's claims of trustworthiness are true. Theoretical evidence has shown that calculus-based trust can be a powerful form of trust to facilitate electronic transactions [34].

## 2.4 Knowledge-based Trust Antecedents

Previous research proposes that trust develops as a result of the aggregation of trust related knowledge by the involved parties [35]. This knowledge is accumulated either first-hand (based on an interaction history) or second-hand. One of the knowledge-based antecedents for trust tested by previous researches is familiarity, an understanding of what, why, where, and when others do what they do [29]. Familiarity emerges as a result of one's learning gained from previous interactions and experiences. It reduces environmental uncertainty by imposing a structure. For example, consumers who are familiar with the site map and the ordering process of a website are more likely to trust the website. In general, familiarity with the situation and various parties involved is found to build trust in business relationships [36]. Past research has found that familiarity with an e-vendor positively influences trust in that e-vendor [37].

## 2.5 Institution-based Trust Antecedent

Institution-based trust means that one believes the necessary impersonal structures are in place to enable one to act in anticipation of a successful future endeavor [36]. Such trust reflects the security one feels about a situation because of guarantees, safety nets, or other structures. The concept of institution-based trust comes from sociology, which deals with the structures (e.g., legal protections) that make an environment feel trustworthy [27]. Two types of institution-based trust have been discussed in the literature: situational normality and structural assurance [36]. Situational normality is an assessment that the success is likely because the situation appears to be normal or favorable. In the context of the Internet, for example, high situational normality would mean that the Internet environment is appropriate, well ordered, and favorable for doing personal business [27]. Structural assurance is an assessment that the success is likely because safeguard conditions such as legal recourse, guarantees and regulations are in place [29, 36, 38]. Prior research has found that institutional-based antecedents positively affect trust in e-vendors [29].

## 2.6 Uncertainty

Uncertainty refers to the degree to which an individual or organization cannot anticipate or accurately predict the environment [39]. Prior research has demonstrated that uncertainty increases transaction cost and decreases acceptance of online purchasing [30]. Uncertainty regarding whether trading parties intend to and will act appropriately is the source of transaction risk which erodes exchange relationships and increases transaction cost [28]. Transaction risks can result from the impersonal nature of the electronic environment. These risks are rooted in two types of uncertainties: about the identity of online trading parties or about the product quality [34]. In the cyber space which lacks security, a dishonest seller can easily masquerade as an honest one to attract an credulous buyer into a fraudulent transaction. In addition, the lack of information about the true quality of the product or service prior to actual purchase makes the buyer more uncertain. One objective of trust building is to reduce the trustor's perceived uncertainty so that transaction cost is lowered and a long-term exchange relationship sustains [40]. Prior studies have stressed the important role of trust in reducing risk or uncertainty in Internet shopping [37]. It has been found that trust mitigates opportunism [41] and information asymmetry [34] in uncertain contexts.

## 2.7 Information Asymmetry

Information asymmetry is defined as the difference between the information possessed by buyers and sellers [34]. Due to information asymmetry, it is difficult and costly for buyers to ascertain the attributes of products and services before purchase. Necessary information regarding quality of products or services may be incomplete or not readily available. Information asymmetry is a problem for Internet shopping due to the physical distance between buyers and sellers. Two sets of agent problems result from information asymmetry: adverse selection and moral hazard [42]. Adverse selection problems take place when the buyer is not capable of knowing the seller's characteristics or the contingencies under which the seller operates. Moral hazard problems occur after a contract is signed, but the seller may misbehave because the buyer is unable to observe its behavior. Marketing researchers have observed that most buyer-seller relationships are characteristic of information asymmetry [43]. When consumers cannot be adequately informed to make a judgment, they are likely to subject to moral hazard and adverse selection problems and perceive a high degree of uncertainty.

## 2.8 Opportunistic Behavior

Opportunistic behavior is prevalent in exchange relationships. In the online buyer-seller relationship, the seller may behave opportunistically by trying to meet its own goals without considering the consumer's benefits. Examples of opportunistic behavior could include misrepresentation of the true quality of a product or service, incomplete disclosure of information, actual quality cheating, contract default, or failure to acknowledge warranties [43]. Some researchers argue that trust can be defined as the expectation that an exchange partner will not engage in opportunistic behavior and one of the consequences of trust is to reduce perceived uncertainty associated with opportunistic behavior [40].

# 3 Wireless Communication Network Perspective

This general perspective of reputation and trust has been applied to the various means and places in so-called "cyber space" where people interact. The most obvious is the realm of e-commerce, which has already been discussed in detail. Other extensions of this style of research in the electronic media include e-mail, electronic social networks such as Friend-of-a-Friend and Friendster, Peer-to-Peer (P2P) systems, and Google's PageRank algorithm [44].

We move from this general perspective, and examine how these broad strokes of research can aid security in a wireless networking environment. Here, as in the more general domain, we find elements of information asymmetry and opportunism. Just as in e-commerce, nodes in MANETs and WSNs have no way of gathering information about nodes beyond their sensing range, and therefore have a great deal of uncertainty. Also, in systems involving asymmetrical duties and designs, some nodes may have different capabilities, allowing them to distribute information that cannot be checked by other nearby nodes.

In addition, the digital, artificial nature of a wireless network both poses new problems and simplifies others. The human brain is a far more complicated and less understood machine than a wireless node. The node is created with certain capabilities, and is limited by such. Whereas a human can imagine and innovate new methods of opportunistic behavior, a node can only perform its programming. But, on the other hand, humans have an evolved sense of reputation and trust that does not require logic to function. We, as designers, must attempt to build reputation and trust networks without the benefit of thousands of years of evolution.

In the following sections, we first give a background on MANETs and WSNs,

and then discuss the challenges in modeling them as reputation and trust-based systems. At the end of this section, we present the various types of node misbehavior.

## 3.1 Background

A MANET is a self-configuring system of mobile nodes connected by wireless links. In a MANET, the nodes are free to move randomly, changing the network's topology rapidly and unpredictably. MANETs are decentralized, and therefore all network activities are carried out by nodes themselves. Each node is both an end-system as well as a relay node to forward packets for other nodes. Such a network may operate as a stand-alone network, or be part of a larger network like the Internet. Since MANETs do not require any fixed infrastructure, they are highly preferred for connecting mobile devices quickly and spontaneously in emergency situations like rescue operations, disaster relief efforts or in other military operations. MANETs can either be managed by an organization that enforces access control or they can be open to any participant that is located closely enough. The later scenario poses greater security threats than the former. In MANETs, more often than not, nodes are individuals and do not have any common interests. It may be advantageous for individual nodes not to cooperate. Hence, they need some kind of incentive and motivation to cooperate. The non-cooperative behavior of a node could be due to selfish intention, for example to save power, or completely malicious intention, for example to launch attacks such as denial-of-service.

A WSN is a network of hundreds and thousands of small, low-power, low-cost devices called sensors. The core application of WSNs is to detect and report events. WSNs have found critical applications in military and civilian life, including robotic landmine detection, battlefield surveillance, environmental monitoring, wildfire detection and traffic regulation. They have been invaluable in saving lives, be it a soldier's life in the battle field or a civilian's life in areas of high risk of natural calamities. In WSNs, all the sensors belong to a single group or entity and work towards the same goal, unlike in MANETs. Also, individual sensors have little value unless they work in cooperation with other sensors. Hence, there is an inherent motivation for nodes in WSNs to be cooperative, and so incentive is less of a concern.

However, since WSNs are often deployed in unattended territories that can often be hostile, they are subject to physical capture by enemies. The obvious solution is to make the nodes themselves tamper-proof. The difficulty with this

solution is that full tamper-proofing makes each individual node prohibitively expensive, and even then does not prevent a truly determined adversary from eventually cracking the node. Since many nodes are often required to cover an area, each node must be economically affordable. As such, simple tamper-proofing is not a viable solution. Hence, sensors can be modified to misbehave and disrupt the entire network. This allows the adversary to access the cryptographic material held by the captured node and allow the adversary to launch attacks from within the system as an insider, bypassing encryption and password security systems. Even though cryptography can provide integrity, confidentiality, and authentication, it fails in the face of insider attacks. This necessitates a system that can cope with such internal attacks.

## 3.2 Node Misbehavior

The intentional non-cooperative behavior of a node, as identified in [14], is mainly caused by two types of misbehavior: *selfish behavior*, e.g., nodes that want to save power, CPU cycles, and memory, and *malicious behavior* which is not primarily concerned with power or any other savings but interested in attacking and damaging the network. When the misbehavior of a node manifests as selfishness, the system can still cope with it since this misbehavior can always be predicted. A selfish node will always behave in a way that maximizes its benefits, and as such, incentive can be used to ensure that cooperation is always the most beneficial option. However, when the misbehavior manifests as maliciousness, it is hard for the system to cope with it, since a malicious node always attempts to maximize the damage caused to the system, even at the cost of its own benefit. As such, the only method of dealing with such a node is detection and ejection from the network.

Malicious misbehavior in packet forwarding can be generally divided into two types of misbehavior, forwarding and routing. Some common forwarding misbehavior are packet dropping, modification, fabrication, timing attacks, and silent route change. Packet dropping, modification, and fabrication are self-explanatory. Timing misbehavior is an attack in which a malicious node delays packet forwarding to ensure that packets expire their Time-To-Live (TTL), so that it is not immediately obvious that it is causing the problem. Silent route changes is an attack in which a malicious node forwards a packet through a different route than it was intended to go through. A malicious node with routing misbehavior attacks during the route discovery phase. Three common attacks of this type are black hole, gray hole, and worm hole. A black-hole attack is one in which a malicious node claims to have the shortest path and then when asked to forward drops the

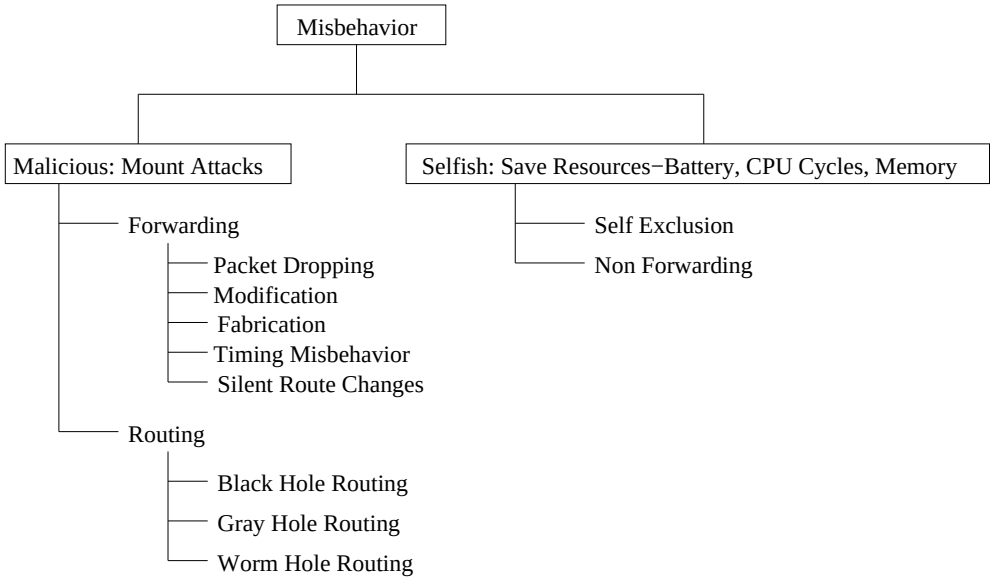


Figure 1: Node Misbehavior

received packets. In a gray-hole attack, which is a variation of the black-hole attack, the malicious node selectively drops some packets. A worm-hole attack, also known as tunneling, is an attack in which the malicious node sends packets from one part of the network to another part of the network, where they are replayed.

The selfish behavior of a node, as shown in Figure 1, can be generally classified as either *self exclusion* or *non-forwarding*. The self-exclusion misbehavior is one in which a selfish node does not participate when a route discovery protocol is executed. This ensures that the node is excluded from the routing list of other nodes. This benefits a selfish node by helping it save its power as it is not required to forward packets for other nodes. A reputation model is an effective way to thwart the intentions of such selfish nodes. Since a node does not forward packets for other nodes in the networks, it is denied any cooperation by other nodes. So, it is in the best interest of a selfish node to be cooperative. On the other hand, the non-forwarding misbehavior is one in which a selfish node fully participates in route discovery phase but refuses to forward the packets for other nodes at a later time. This selfish behavior of a node is functionally indistinguishable from a malicious packet dropping attack.

Since reputation-based systems can cope with any kind of observable mis-

behavior they are useful in protecting a system. Reputation and trust-based systems enable nodes to make informed decisions on prospective transaction partners. Researchers have been steadily making efforts to successfully model WSNs and MANETs as reputation and trust-based systems. Adapting reputation and trust-based systems to WSNs presents greater challenges than MANETs and Peer-to-Peer (P2P) systems due to their energy constraints. CORE [15], CONFIDANT [12], RFSN [23], DRBTS [26], KeyNote [3], and RT Framework [16] are a few successful attempts. However, RFSN and DRBRTS are the only works so far focusing on WSNs. The others concentrate on MANETs and P2P networks.

# 4 Reputation and Trust-based Systems

Reputation and trust-based system have now been used for over half a decade for internet, e-commerce, and P2P systems [4, 5, 7, 8, 11]. More recently, efforts have been made to model MANETs and WSNs as reputation and trust-based systems [6, 12, 14, 19]. In this section we will discuss the various aspects of reputation and trust-based systems. To begin with, we present the goals of a reputation and trust-based system. Then, we discuss the properties of reputation and trust-based systems including the properties of reputation and trust metrics. Then we discuss various types of system initialization followed by different classifications of reputation and trust-based systems. Finally, we end the section with a discussion of the pros and cons of reputation and trust-based systems.

## 4.1 System Goals

The main goals of reputation and trust-based systems, as identified in [7], after adapting them to wireless communication networks, are as follows:

- Provide information that allows nodes to distinguish between trustworthy and non-trustworthy nodes.
- Encourage nodes to be trustworthy.
- Discourage participation of nodes that are untrustworthy.

In addition, we have identified two more goals of a reputation and trust-based system from a wireless communication network perspective. The first goal is to cope with any kind of observable misbehavior. The second goal is to minimize the damage caused by insider attacks.

## 4.2 Properties

To operate effectively, reputation and trust-based systems require at least three properties, as identified in [4].

- Long-lived entities that inspire an expectation of future interaction.
- The capture and distribution of feedback about current interactions (such information must be visible in the future).
- Use of feedback to guide trust decisions.

The trust metric itself has the following properties.

- Asymmetric: Trust is not symmetric, i.e., if node A trusts node B, then it is not necessarily true that node B also trusts node A.
- Transitive: Trust is transitive, i.e., if node A trusts node B and node B trusts node C, then node A trusts node C.
- Reflexive: Trust is reflexive, i.e., a node always trusts itself.

## 4.3 Initialization

Reputation and trust-based systems can be initialized in one of the following ways. 1) All nodes in the network are considered to be trustworthy. Every node trusts every other node in the network. The reputation of the nodes is decreased with every bad encounter. 2) Every node is considered to be untrustworthy and no node in the network trusts any other node. The reputation of nodes with such an initialization system is increased with every good encounter. 3) Every node in the network is neither considered trustworthy nor untrustworthy. They all take a neutral reputation value to begin with. Then with every good or bad behavior, the reputation value is increased or decreased, respectively.

## 4.4 Classification

We have recognized that reputation and trust-based systems can be broadly classified by the following groups.

1. Observation

- First-hand: The system uses direct observation or its own experience to update reputation.
- Second-hand: The system uses information provided by peers in its neighborhood.

Most systems proposed so far use both first-hand and second-hand information to update reputation. This allows the system to make use of the experience of its neighbors to form its opinions. Some systems choose not to use both types of information. In systems that use only first hand information, a node's reputation value of another node is not influenced by others. This makes the system completely robust against rumor spreading. OCEAN and *pathrater* [6] are two such systems that make use of only first-hand information. Only one system so far, DRBTS, has the unique situation where a certain type of node uses only second-hand information. In this system, a node does not have any first-hand information to evaluate the truthfulness of the informers. One way to deal with this situation is to use a simple majority principle.

2. Information Symmetry

   - Symmetric: All nodes in the network have access to the same amount of information, i.e., both first-hand and second-hand. When making a decision, no node has more information than any other node.
   - Asymmetric: All nodes do not have access to the same amount of information. For example, in DRBTS[26], sensor nodes do not have first-hand information. Thus, in the decision making stage, the sensor nodes are at a disadvantage.

3. Centralization

   - Centralized: One central entity maintains the reputation of all the nodes in the network, for example like in eBay or YAHOO auctions. Such a reputation system can cause both a security and information bottleneck.
   - Distributed: Each node maintains the reputation information of all the nodes it cares about. In this kind of a reputation system, there could be issues concerning the consistency of reputation values at different nodes, i.e., there may not be a consistent local view. Each node can have either local or global information.

- Local: Nodes have reputation information only of nodes in their neighborhood. This is the most reasonable option, particularly for static sensor networks, since nodes interact only with their immediate neighbors. This mitigates memory overhead to a large extent.
- Global: Nodes have reputation information of all the nodes in the network. This is suitable for networks with lots of node mobility. Even after moving to a new location, nodes are not completely alienated and have a reasonable understanding of their new neighborhood. Unfortunately, this leads to a large overhead, and can lead to scalability problems.

### 4.5 Pros and Cons

Reputation and trust-based systems are one of the best solutions for dealing with selfish misbehavior. They are also very robust solutions to curtail insider attacks. Reputation and trust-based systems are, for the most part, self maintaining. Unfortunately, along with the added overhead, both in computation and communication, they also add another dimension of security consideration. Now, an adversary has another vector to attack the system with, the reputation system itself. It is difficult to properly design the reputation system in order to make it robust enough to survive such attacks, but we will examine that trade-off a little later in the chapter.

## 5 Components

This section is dedicated completely to an in depth discussion of the various components of reputation and trust-based systems. We have identified four important components in a reputation and trust-based system: information gathering, information sharing, information modeling, and decision making. In the rest of this section we will discuss each of these components in detail, presenting examples of real world systems whenever appropriate.

### 5.1 Information Gathering

Information gathering is the process by which a node collects information about the nodes it cares about. This component of the reputation and trust-based Systems is concerned only with first-hand information. First-hand information is the

information gathered by a node purely based on its observation and experience. However, according to CONFIDANT[12], first-hand information can be further classified into *personal experience* and *direct observation*. Personal experience of a node refers to the information it gathers through one-to-one interaction with its neighboring nodes. On the other hand, direct observation refers to the information a node gathers by observing the interactions among its neighboring nodes. CONFIDANT is currently the only system to make this distinction.

Most reputation and trust-based systems make use of a component called *watchdog* [6] to monitor their neighborhood and gather information based on promiscuous observation. Hence, first-hand information is confined to the wireless sensing range of a node. However, the watchdog system is not very effective in the case of directional antennas, limiting its broad application, especially in very secure situations. This limitation has received very little study currently.

## 5.2 Information Sharing

This component of reputation and trust-based systems is concerned with dissemination of first-hand information gathered by nodes. There is an inherent trade-off between efficiency in using second-hand information and robustness against false ratings. Using second-hand information has many benefits. The reputation of nodes builds up more quickly, due to the ability of nodes to learn from eachothers' mistakes. No information in the system goes unused. Using second-hand information has an additional benefit, in that over time, a consistent local view will stabilize.

However, sharing information comes at a price. It makes the system vulnerable to false report attacks. This vulnerability can be mitigated by adopting a strategy of limited information sharing, i.e., sharing either only *positive information* or *negative information*.

The difficulty with the solution is that while sharing only positive information limits the vulnerability of the system to false praise attacks, it has its own drawbacks. When only positive information is shared, not all the information in the system is used, since nodes cannot share their bad experiences. This is particularly detrimental since learning from ones own experience in this scenario comes at a very high price. Also, colluding malicious nodes can extend each other's survival time through false praise reports. CORE [14] suffers from this attack.

Similarly, sharing only negative information prevents the false praise attack mentioned above, but has its own drawbacks. Not all the information in the sys-

tem is used, since nodes cannot share their good experiences. More importantly, malicious nodes can launch a bad-mouth attack on benign nodes either individually or in collusion with other malicious nodes. CONFIDANT [12] suffers from this attack.

Yet another way of avoiding the negative consequences of information sharing is to not share information at all. OCEAN [17] is one such model that builds reputation purely based on its own observation. Such systems, though they are completely robust against rumor spreading, have some serious drawbacks. The time required for the system to build reputation is increased dramatically, and it takes longer for reputation to fall, allowing malicious nodes to stay in the system longer.

Systems like DRBTS [26] and RFSN [23] share both positive and negative information. The negative effects of information sharing, as discussed above, can be mitigated by appropriately incorporating first-hand and second-hand information into the reputation metric. Using different weighting functions for different information is one efficient techniques.

With respect to information sharing, we have identified three ways in which information can be shared among nodes: *friends list*, *blacklist*, and *reputation table*. A friends list shares only positive information, a blacklist shares only negative information, while a reputation table shares both positive and negative information.

For sharing information, three important issues have to be addressed: dissemination frequency, dissemination locality, and dissemination content.

Dissemination frequency can be classified into two types:

- Proactive Dissemination: In proactive dissemination, nodes publish information during each dissemination interval. Even if there has been no change to the reputation values that a node stores, it still publishes the reputation values. This method is suitable for dense networks to prevent congestion since they have to wait till the dissemination interval to publish.

- Reactive Dissemination: In reactive dissemination, nodes publish only when there is a predefined amount of change to the reputation values they store or when an event of interest occurs. This method mitigates the communication overhead in situations where there is not frequent updates to the reputation values. However, reactive dissemination may cause congestion in dense networks with high network activity, or cause the system to stall if network activity is especially low.

In both these types of information dissemination, the communication overhead can be mitigated to a large extent by piggy backing the information with other network traffic. For example, in CORE, the reputation information is piggy backed on the reply message and in DRBTS it is piggy backed on the location information dispatch.

Dissemination locality can be classified into two types:

- Local: In local dissemination, the information is published within the neighborhood. It could be either through a local broadcast, multicast or unicast. In DRBTS [26], the information is published in the neighborhood through a local broadcast. This enables all the beacon nodes to update their reputation table accordingly. Other models may choose to unicast or multicast depending on the application domain and security requirements.

- Global: In global dissemination, the information is sent to nodes outside the range of the publishing node. Like local dissemination, global dissemination could use one of the three publishing techniques: broadcast, multicast or unicast. For networks with node mobility, global dissemination is preferred since this gives nodes a reasonable understanding of the new location they are moving to.

Content of information disseminated can be classified into two types:

- Raw: The information published by a node is its first-hand information only. It does not reflect the total reputation value, which includes the second-hand information of other nodes in the neighborhood. Disseminating raw information prevents information from looping back to the originator.

- Processed: The information published by a node is its overall opinion of the nodes in its reputation tables. This includes information provided to the node by others in the neighborhood.

## 5.3 Information Modeling

This component of a reputation and trust-based system deals with combining the first-hand and second-hand information meaningfully into a metric. It also deals with maintaining and updating this metric. Some models choose to use a single metric, reputation, like CORE and DRBTS [14, 26] while a different model like

RFSN may choose to use two separate metrics, reputation and trust, to model the information [23]. While most models make use of both first-hand and second-hand information in updating reputation and/or trust, some models like OCEAN [17] may use just first-hand information. The first-hand information can be directly incorporated into the reputation metric without much processing.

However, this is not the case with second-hand information. The node providing the second-hand information could be malicious and ratings it provides could be spurious. Hence it is necessary to use some means of validating the credibility of the reporting node. One method is to use a deviation test like in [21, 26]. If the reporting node qualifies the deviation test, then it is treated as trustworthy and its information is incorporated to reflect in the reputation of the reported node. However, different models may choose to use a different strategy in accepting the second-hand information depending on the application domain and security requirements. For instance, the model in [23] uses Dempster-Shafer belief theory [2] and discounting belief principle [9] to incorporate second-hand information. However, Beta distribution has been the most popular among researchers in reputation and trust-based systems. It was first used by Josang and Ismail [11]. Since then, many researchers have used the beta distribution including Ganeriwal and Srivastava [23] and Buchegger and Boudec [21]. Beta distribution is the simplest among the various distribution models, viz poison, binomial or Gaussian, that can be used for representation of reputation. This is mainly because of the fact that it is indexed by only two parameters.

An important issue in maintaining and updating reputation is how past and current information is weighted. Different models tend to weight them differently, each with a different rationale. Models like CORE tend to give more weight to the past observations with the argument that a more recent sporadic misbehavior should have minimal influence on a nodes reputation that has been built over a long period of time. This helps benign nodes that are selfish due to genuinely critical battery conditions. Also, occasionally, nodes may temporarily misbehave due to technical problems like link failure in which case it is justified not to punish them severely.

On the other hand, models like RFSN tend to give more weight to recent observations than the past, with the argument that a node has to contribute and cooperate on a continuous basis to survive. This is known as aging, where old observations have little influence on a node's current reputation value. This forces nodes to be cooperative at all times. Otherwise, a malicious node will build its reputation over a long period and then start misbehaving by taking advantage of its accumu-

lated goodness. The higher the reputation a malicious node builds, the longer it can misbehave before it can be detected and excluded. However, there is a drawback in adopting the aging technique. In periods of low network activity, a benign node gets penalized. This can be resolved by generating network traffic in regions and periods of low network activity using mobile nodes. DRBTS resolves this problem with beacon nodes being capable of generating network traffic on a need basis.

### 5.4 Decision Making

This component of a reputation and trust-based system is responsible for taking all the decisions. The decisions made by this component are based on the information provided by the information modeling component. The basic decision is a binary decision, on who to trust and who not to. The actual decision could translate to be one of cooperate/don't-cooperate, forward/don't-forward, etc, based on the function being monitored by the system.

The decision of this component varies along with the reputation and trust values in the information modeling component. The decision can vary from trust to no-trust, wherein a node that was trusted so far will no longer be trusted after its reputation and trust values fall below a predetermined threshold. Similarly it can vary from no-trust to trust, wherein a node that was initially not trusted will be trusted soon after its reputation and trust values exceed a predetermined threshold.

## 6 Examples of Reputation and Trust-based Models"

In this section we will review various reputation and trust-based models that have been proposed for MANETs and WSNs over the last few years. For each model, we will review the working principle, in light of the discussions presented in the previous sections.

### 6.1 CORE

CORE stands for "A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks". This model was proposed by Michiardi and Molva [15] to enforce node cooperation in MANETs based on a collaborative monitoring technique. CORE is a distributed, symmetric reputation model

which uses both first-hand and second-hand information for updating reputation values. It uses bi-directional communication symmetry and dynamic source routing (DSR) protocol for routing. CORE also assumes wireless interfaces that support promiscuous mode operation.

In CORE, nodes have been modeled as members of a community and have to contribute on a continuing basis to remain trusted, else their reputation will degrade until eventually they are excluded from the network. The reputation is formed and updated along time. CORE uses three types of reputation, namely *subjective reputation*, *indirect reputation*, and *functional reputation* and addresses only the selfish behavior problem. CORE assigns more weight to the past observations than the current observations. This ensures that a more recent sporadic misbehavior of a node has minimum influence on the evaluation of overall reputation value of that node. CORE has two types of protocol entities, a requestor and a provider.

- Requestor: refers to a network entity asking for the execution of a function $f$. A requestor may have one or more providers within its transmission range.
- Provider: refers to any entity supposed to correctly execute the function $f$.

In CORE, nodes store the reputation values in a reputation table (RT), with one RT for each function. Each entry in the RT corresponds to a node and consists of four entries: unique ID, recent subjective reputation, recent indirect reputation, and composite reputation for a predefined function. Each node is also equipped with a watchdog mechanism for promiscuous observation. RTs are updated in two situations: during the request phase and during the reply phase.

**Information Gathering:** The reputation of a node computed from first-hand information is referred to as subjective reputation . It is calculated directly from a node's observation. CORE does not differentiate between interactions and observation for subjective reputation unlike CONFIDANT [12]. The subjective reputation is calculated only for the neighboring nodes, i.e., nodes in the transmission range of the subject. The subjective reputation is updated only during the request phase. If a provider does not cooperate with a requestor's request, then a negative value is assigned to the rating factor $\sigma$ of that observation and consequently the reputation of the provider will decrease. The reputation value varies between -1 and 1. New nodes, when they enter the network, are also assigned a neutral reputation value of $0$ since enough observations are not available to make an assessment of their reputation.

**Information Sharing:** CORE uses indirect reputation, i.e., second-hand information, to model MANETs as complex societies. Thus, a node's impression of another node is influenced by the impression of other members of the society. However, there is a restriction imposed by CORE on the type of information propagated by the nodes. Only positive information can be exchanged. As we have stated before, this prevents bad mouthing attacks on benign nodes. It is assumed that each reply message consists of a list of nodes that cooperated. Hence indirect reputation will be updated only during the reply phase.

**Information Modeling:** CORE uses functional reputation to test the trustworthiness of a node with respect to different functions. Functional reputation is the combined value of subjective and indirect reputation for different functions. Different applications may assign different weight to routing and similarly to various other functions like packet forwarding, etc.

The authors argue that reputation is compositional, i.e., the overall opinion on a node that belongs to the network is obtained as a result of the combination of different type of evaluations. Thus, the global reputation for each node is obtained by combining the three types of reputation.

Finally, reputation values that are positive are decremented along time to ensure that nodes cooperate and contribute on a continuing basis. This prevents a node from initially building up a good reputation by being very cooperative and contributive but abuse the system later.

**Decision Making:** When a node has to make a decision on whether or not to execute a function for a requestor, it checks the reputation value of that node. If the reputation value is positive, then it is a well behaved entity. On the other hand, if the reputation value of the requestor is negative, then it is tagged as a misbehaving entity and denied the service. A misbehaving entity is denied service unless it cooperates and ameliorates its reputation to a positive value. Reputation is hard to build, because reputation gets decreased every time the watchdog detects a non cooperative behavior and it also gets decremented along time to prevent malicious nodes from building reputation and then attacking the system resources.

**Discussions:** Giving greater weight to the past does enable a malicious node to misbehave temporarily if it has accumulated a high reputation value. Since only positive information is shared for indirect reputation updates, CORE prevents false accusation attacks, confining the vulnerability of the system to only false praise. The authors argue that a misbehaving node has no advantage by giving false praise to other unknown entities. This is true only so long as malicious nodes are not colluding. When malicious nodes start collaborating, then they can help

prolong the survival time of one another through false praise. However, the effect of false praise is mitigated in CORE to some extent by coupling the information dissemination to reply messages. Also, since only positive information is shared, the possibility of retaliation is prevented.

There is an inherent problem in combining the reputation values for various functions into a single global value. This potentially helps a malicious node to hide its misbehavior with respect to certain functions by behaving cooperatively with respect to the remaining functions. The incentive for a node to misbehave with respect to a particular function is to save scarce resource. The node may choose to not cooperate for functions that consume lots of memory and/or power and choose to cooperate for functions that don't require as much memory and/or power. Nonetheless, functional reputation is a very nice feature of CORE that can be used to exclude nodes from functions for which their reputation value is below the threshold and include them for functions for which their reputation value is above the threshold.

CORE also ensures that disadvantaged nodes that are inherently selfish due to their critical energy conditions are not excluded from the network using the same criteria as for malicious nodes. Hence, an accurate evaluation of the reputation value is performed that takes into account sporadic misbehavior. Therefore, CORE minimizes false detection of a nodes misbehavior.

## 6.2 CONFIDANT

CONFIDANT stands for "Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks". This model was proposed by Buchegger and Boudec [12] to make misbehavior unattractive in MANETs based on selective altruism and utilitarianism. CONFIDANT is a distributed, symmetric reputation model which uses both first-hand and second-hand information for updating reputation values. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. In CONFIDANT, Dynamic Source Routing (DSR) protocol has been used for routing and it assumes a promiscuous mode operation. CONFIDANT also assumes that no tamper-proof hardware is required for itself, since a malicious node neither knows its reputation entries in other nodes nor has access to other nodes to modify their values. CONFIDANT is inspired by "The Selfish Gene" by Dawkins [1] which states reciprocal altruism is beneficial for every ecological system when favors are returned simultaneously because of instant gratification. The benefit of behaving well is not so obvious in the case where there is

a delay between granting a favor and the repayment. The CONFIDANT protocol consists of four components at each node: Monitor, Trust Manager, Reputation System, and Path Manager.

**Information Gathering:** The Monitor helps each node in passively observing their 1-hop neighborhood. Nodes can detect deviations by the next node on the source route. By keeping a copy of a packet while listening to the transmission of the next node, any content change can also be detected. The monitor registers these deviations from normal behavior and as soon as a given bad behavior occurs, it is reported to the reputation system. The monitor also forwards the received ALARMS to the Trust Manager for evaluation.

**Information Sharing:** The Trust Manager handles all the incoming and outgoing ALARM messages. Incoming ALARMs can originate from any node. Therefore, the source of an ALARM has to be checked for trustworthiness before triggering a reaction. This decision is made by looking at the trust level of the reporting node. CONFIDANT has provisions for several partially trusted nodes to send ALARMs which will be considered as an ALARM from a single fully trusted node. The outgoing ALARMS are generated by the node itself after having experienced, observed, or received a report of malicious behavior. The recipients of these ALARM messages are called friends, which are maintained in a friends list by each node.

The trust manager consists of the three components: *alarm table*, *trust table*, and *friends list*. An alarm table contains information about received alarms. A trust table manages trust levels for nodes to determine the trustworthiness of an incoming alarm. A friends list has all friends a node has to which it will send alarms when a malicious behavior is observed. The Trust Manager is also responsible for providing or accepting routing information, accepting a node as part of a route, and taking part in a route originated by some other node.

**Information Modeling:** The Reputation System manages a table consisting of entries for nodes and their rating. Ratings are changed only when there is sufficient evidence of malicious behavior that has occurred at least a threshold number of times to rule out coincidences. The rating is then changed according to a rate function that assigns the greatest weight for personal experience, a smaller weight for observations in the neighborhood and an even smaller weight to reported experience. Buchegger and Boudec state that the rationale behind this weighting scheme is that nodes trust their own experiences and observations more than those of other nodes. Then, the reputation entry for the misbehaving node is updated accordingly. If the entry for any node in the table falls below a predeter-

mined threshold, then the Path Manager is summoned.

**Decision Making:** The *Path Manager* is the component that is the decision maker. It is responsible for path re-ranking according to the security metric. It deletes paths containing misbehaving nodes and is also responsible for taking necessary actions upon receiving a request for a route from a misbehaving node.

**Discussions:** In CONFIDANT only negative information is exchanged between nodes and the authors argue that it is justified since malicious behavior will ideally be the exception not the normal behavior. However, since only negative information is exchanged, the system is vulnerable to false accusation of benign nodes by malicious nodes. Unlike in CORE, even without collusion, malicious nodes benefit by falsely accusing benign nodes. With collusion of malicious nodes, this problem can explode beyond control. However, false praise attacks are prevented in CONFIDANT since no positive information is exchanged. This eliminates the possibility of malicious nodes colluding to boost the survival time of one another. Also, since negative information is shared between nodes, an adversary gets to know his situation and accordingly change his strategy. This may not be desirable. Sharing negative information in the open also introduces fear of retaliation which may force nodes to withhold their true findings.

In CONFIDANT, despite designing a complete reputation system, the authors have not explained how the actual reputation is computed and how it is updated using experienced, observed and reported information. Also, in CONFIDANT, nodes that are excluded will recover after a certain timeout. This gives malicious nodes a chance to reenter the system and attack repeatedly unless they are revoked after a threshold number of reentries. Failed nodes in CONFIDANT are treated like any other malicious node which is both good and bad. It is good, because any node that is uncooperative should be punished, but it is bad because a genuine node may not be able to cooperate due to a temporary problem, and punishment may make it even worse. Also, the authors have not provided any evidence to support their rationale behind differentiating first-hand information as personal experience and direct observation and assigning them different weights.

## 6.3 Improved CONFIDANT- Robust Reputation System

Buchegger and Boudec presented an improved version of CONFIDANT [21]. They called this "A Robust Reputation System" (RRS). The RRS was an improvement on CONFIDANT introducing a Bayesian framework with Beta distribution to update reputation. Unlike in CONFIDANT, the RRS uses both positive and

negative reputation values in the second-hand information.

The RRS uses two different metrics: reputation and trust. The reputation metric is used to classify other nodes as normal/misbehaving while the trust metric is used to classify other nodes as trustworthy/untrustworthy. Whenever second-hand information is received from a node, the information is subjected to a deviation test. If the incoming reputation information does not deviate too much from the receiving node's opinion, then the information is accepted and integrated. Since the reporting node sent information the receiver sees as valid, the reporting node's trust rating is increased. On the other hand, if the reputation report deviates past the threshold, then the reporting node's trust value is lowered. The receiving node also decides whether to integrate the deviating information or not, depending on whether the reporting node is trusted or untrusted, respectively. To use a real world example, if a trusted friend tells us something that is counter to our experience, we give the benefit of the doubt, but too many such deviations will cause us to lose our trust in the friend.

In RRS, only fresh information is exchanged. Unlike CORE, RRS gives more weight to current behavior than the past. The authors argue that, if more weight is given to past behavior, then a malicious node can choose to be good initially till it builds a high reputation and trust value and then choose to misbehave. By assigning more weight to current behavior, the malicious node is forced to cooperate on a continuing basis to survive in the network.

## 6.4 RFSN

RFSN stands for Reputation-based Framework for Sensor Networks. This model was proposed by Ganeriwal and Srivastava [23]. RFSN is a distributed, symmetric reputation-based model that uses both first-hand and second-hand information for updating reputation values. In RFSN, nodes maintain the reputation and trust values for only nodes in their neighborhood. The authors argue that there exists no sensor network application in which a node will require prior reputation knowledge about a node many hops away. The objective of RFSN is to create a community of trustworthy sensor nodes. RFSN was the first reputation and trust-based model designed and developed exclusively for sensor networks. RFSN distinguishes between trust and reputation and uses two different metrics.

From Figure 2, it is clear that the first-hand information from the watchdog mechanism and second hand information are combined to get the reputation value of a node. Then the trust level of a node is determined from its reputation. Fi-

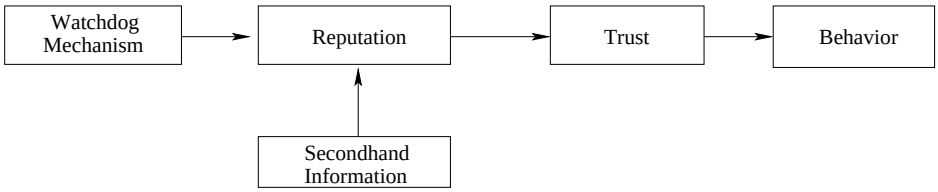


Figure 2: Architectural Design of RFSN [23]

nally, based on the trust value, the node's behavior towards the node in question is determined. If the trust value is above a certain threshold, then the behavior is "cooperate", else it is "don't cooperate".

**Information Gathering:** RFSN, like many other systems, uses a watchdog mechanism for first-hand information. In RFSN, the watchdog mechanism consists of different modules, typically one for each function it wants to monitor. The higher the number of modules, the greater the resource requirements. RFSN maintains the reputation as a probabilistic distribution which gives it complete freedom, unlike a discrete value. The authors argue that reputation can only be used to statistically predict the future behavior of other nodes and it cannot deterministically define the action performed by them. The reputation of all nodes that node $i$ interacts with is maintained in a reputation table.

The direct reputation, $(R_{ij})_D$, is updated using the direct observations, i.e., the output of the watchdog mechanism.

**Information Sharing:** In RFSN, nodes share their findings with fellow nodes. However, they are allowed to share only positive information. RFSN gives higher weight to second-hand information from nodes with higher reputation, which is reasonable and fairly novel. The weight assigned by node $i$ to second-hand information from a node $k$ is a function of the reputation of node $k$ maintained by node $i$. Like many other reputation and trust based systems, RFSN also makes use of the popular Beta distribution model.

**Information Modeling:** Assume node $i$ has established some reputation value, $R_{ij}$, for node $j$. Let the two nodes have $r + s$ more interactions with $r$ cooperative and $s$ non-cooperative interactions respectively. The reputation value is now updated as follows.

$$R_{ij} = Beta(\alpha_j^{new} + 1, \beta_j^{new} + 1) \tag{1}$$

$$\alpha_j^{new} = (w_{age} * \alpha_j) + r \tag{2}$$

$$\beta_j^{new} = (w_{age} * \beta_j) + s \tag{3}$$

RFSN, unlike CORE, gives more weight to recent observations. This is done by using $w_{age}$, which is range bound in the space(0,1). This is for updating reputation value using direct observation.

To update the reputation value using second-hand information, RFSN maps the problem into the Dempster-Shafer belief theory[1] [2] domain. Then, the problem is solved using the belief discounting theory [9]. Using this theory, the reputation of the reporting node is automatically taken into account in the calculation of the reputation of the reported node. Hence, a separate deviation test is not necessary. A node with higher reputation gets higher weight than a node with lower reputation. Then, the trust level of a node is determined using its reputation value. It is determined as the statistically expected value of the reputation.

**Decision Making:** Finally, in the decision making stage, node $i$ has to make a decision on whether or not to cooperate with node $j$. The decision of node $i$ is referred to as its behavior $B_{ij}$ and is a binary value: $\{$cooperate, don't cooperate$\}$. Node $i$ uses $T_{ij}$ to make a decision as follows.

$$B_{ij} = \begin{cases} cooperate & \forall T_{ij} \geq B_{ij} \\ don't\ cooperate & \forall T_{ij} < B_{ij} \end{cases} \tag{4}$$

**Discussions:** Like CONFIDANT, RFSN also treats misbehaving and faulty nodes the same way. The rationale is that a node that is uncooperative has to be excluded irrespective of the cause of uncooperative behavior. In RFSN, nodes are allowed to exchange only good reputation information. Also, in RFSN, only direct reputation information is propagated. This prevents the information from looping back to the initiating node. However, this increases the memory overhead slightly since a separate data structure has to be maintained for direct reputation.

## 6.5 DRBTS

DRBTS stands for "Distributed Reputation and trust-based Beacon Trust System". This model was proposed by Srinivasan, Teitelbaum and Wu recently to solve a

[1]The Dempster-Shafer theory is a mathematical theory of evidence used to combine different pieces of information to calculate the probability of an event. It is a generalization of the Bayesian theory of subjective probability.

special case in location-beacon sensor networks. DRBTS is a distributed model that makes use of both first-hand and second-hand information. It has two types of nodes: beacon node (BN) and sensor node (SN). It is symmetric from the BN perspective but asymmetric from the SN perspective. This is because beacon nodes are capable of determining their location, and must pass this information to the sensor nodes. The difficulty is that without knowledge of their own location, a sensor node has no way of telling if a beacon node is lying to it. DRBTS enables sensor nodes to exclude location information from malicious beacon nodes on the fly by using a simple majority principle. DRBTS addresses the malicious misbehavior of beacon nodes.

**Information Gathering:** In DRBTS, information gathering is addressed from two different perspectives: the sensor node perspective and the beacon node perspective. From a beacon node perspective, DRBTS uses a watchdog for neighborhood watch. When a SN sends a broadcast asking for location information, each BN will respond with its location and the reputation values for each of its neighbors. The watchdog packet overhears the responses of the neighboring beacon nodes. It then determines its location using the reported location of each BN in turn, and then compares the value against its true location. If the difference is within a certain margin of error, then the corresponding BN is considered benign, and its reputation increases. If the difference is greater than the margin of error, then that BN is considered malicious and its reputation is decreased. From a sensor node perspective, there is no first-hand information gathered by sensor nodes through direct observations. They rely completely on the second-hand information passed to them from nearby beacon nodes during the location request stage.

DRBTS also includes a method by which BNs can send out location requests disguised as SNs, in case of low network activity. However, unlike CONFIDANT, DRBTS does not differentiate first-hand information into personal experience and direct observation.

**Information Sharing:** DRBTS does make use of second-hand information to update the reputation of its neighboring nodes. However, information sharing is only with respect to BNs. SNs do not share any information since they do not collect any by virtue of their own observation of their neighborhood. In DRBTS, nodes are allowed to share both positive and negative reputation information. This is allowed to ensure a quick learning time.

**Information Modeling:** Let BN $j$ respond to a SN's request. Then BN $i$, in the range of $j$ updates its reputation entry of $j$ using using this direct observation

as follows.

$$R_{ki}^{New} = \mu_1 \times R_{ki}^{Current} + (1 - \mu_1) \times \tau \tag{5}$$

where $\tau = 1$ if the location was deemed to be truthful and $\tau = 0$ otherwise, and $\mu_1$ is a weight factor.

To use second-hand information, assume B$j$ is reporting about BN $k$ to BN $i$. Now BN $i$ first performs a deviation test to check if the information provided by BN $j$ is compatible.

$$|R_{ji}^{Current} - R_{ki}^{Current}| \leq d. \tag{6}$$

If the above test is positive, then information provided is considered to be compatible and the entry $R_{ik}$ is updated as follows.

$$R_{j,i}^{New} = \mu_2 \times R_{j,i}^{Current} + (1 - \mu_2) \times R_{k,i}^{Current}. \tag{7}$$

But, if the deviation test in equation 6 is negative, then $j$ is considered to be lying and its reputation is updated as follows.

$$R_{j,k}^{New} = \mu_3 \times R_{j,k}^{Current}. \tag{8}$$

Equation 8 ensures that nodes that lie are punished so that such misbehavior can be discouraged.

**Decision Making:** Decisions are made from the sensor node's perspective. A SN, after sending out a location request waits until a predetermined timeout. A BN has to reply before the timeout with its location information and its reputation ratings for its neighbors. Then, the SN, using the reputation ratings of all the responding BNs, tabulates the number of positive and negative votes for each BN in its range. Finally, when the SN has to compute its location, it considers the location information only from BNs with positive votes greater than negative votes. The remaining location information is discarded.

**Discussions:** DRBTS addresses the malicious misbehavior of beacon nodes. This unique problem that this system solves, though very important to a specific branch of WSNs, is not encountered very frequently . However, the idea can be easily extended to other problem domains.

# 7 Open Problems

Though lots of research has been done in this field, reputation and trust-based systems are still in their incubation phase when it comes to MANETs and WSNs.

There are some open problems that have been identified which need to be resolved sooner, rather than later. One such problem is the bootstrap problem. It takes a while to build reputation and trust among nodes in a network. Minimizing this startup period is still an open issue. Using all the available information does help in building reputation and trust among nodes quickly, but as examined earlier, it makes the system vulnerable to false report attacks. Also, in systems like CORE where nodes have to contribute on a continued basis to survive, periods and regions of low network activity pose new problems. Aging will deteriorate the reputation of even benign nodes since there is no interaction.

Another important problem that needs to be addressed is the intelligent adversary strategies. An intelligent adversary can manifest the degree of his misbehavior such that he can evade the detection system. A game theoretic approach to resolve this problem may be a worthy investigation.

A system like CORE uses functional reputation to monitor the behavior of nodes with respect to different functions. However, CORE unifies the reputation of a node for various functions into a global reputation value of that node. This may not be very effective since it will allow an adversary to cover his misbehavior with respect to one function by being well behaved for other functions. No literature so far has addressed the benefits of using functional reputation values independently. It may be beneficial to exclude nodes for a particular function if it is known for misbehaving with respect to that function rather than judging him with respect to over behavior. For example, a specific lawyer might be known to be a great person to have on your side if you need a case dismissed, while being known to cheat at cards. Knowing this, you would hire him to argue a case, but perhaps not invite him to the weekly poker game.

Finally, a scheme needs to be developed to motivate nodes to publish their ratings honestly. This is particularly important for MANETs since nodes often don't belong to the same entity. However, in WSNs, since nodes tend to belong to some overarching system, there is an inherent motivation for nodes to participate honestly in information exchange. Market schemes seem to show some promise in similar problems in routing in P2P and MANETs, and inspiration might be drawn from these fields.

# 8 Conclusion

Reputation and trust are two very important tools that have been used since the beginning to facilitate decision making in diverse fields from an ancient fish market

to state of the art e-commerce. This chapter has provided a detailed understanding of reputation and trust-based systems both from a societal as well as a wireless communication networks' perspective. We have examined all aspects of reputation and trust-based systems including their goals, properties, initialization and classification. Also, we have have provided an in depth discussion of the components of reputation and trust-based systems. A comprehensive review of research works focusing on adapting reputation and trust-based systems to MANETs and WSNs has been presented, along with an in depth discussion of their pros and cons. We have also presented some open problems that are being researched even now.

# 9 Acknowledgements

This work was supported in part by NSF grants ANI 0073736, EIA 0130806, CCR 0329741, CNS 0422762, CNS 0434533, and CNS 0531410.

# 10 Exercises

Answering the following questions will help you in evaluating your level of understanding of the material presented in this chapter.

1. Discuss any two areas of application of reputation and trust-based systems with respect to ad-hoc and sensor networks other than those discussed in this chapter.

2. How can the bootstrap problem in reputation and trust-based systems be efficiently addressed?

3. Information asymmetry plays a critical role. Discuss one situation in details, other than those presented in this chapter where Information asymmetry plays a vital role.

4. In all the systems discussed in this chapter, the reputation and trust metric have been considered to be either black or white, i.e., either an entity has good reputation or bad reputation, an entity is either trusted or not trusted. However, in real life there is an element of uncertainty. Discuss a reputation and trust-based model which incorporates uncertainty into the reputation and trust metrics.

5. Can you think of any real life metric other than reputation and trust onto which mobile ad-hoc and sensor network security problems can be mapped and solved?

# References


[1] R. Dawkins. The Selfish Gene. *Oxford University Press*, 1989 edition, (First Edition was 1976).

[2] G. Shafer. A mathematical theory of evidence. *Princeton University*, 1976.

[3] M. Blaze, J. Feigenbaum, J. Ioannidis and A. Keromytis. RFC2704 - The KeyNote Trust Management System Version 2. 1999.

[4] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation systems. *Communications of the ACM*, 43(12):4548, 2000.

[5] C. Dellarocas. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. *In Proceedings of the ACM Conference on Electronic Commerce*, pages 150157, 2000.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. *In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000)*.

[7] P. Resnick and R. Zeckhauser. Trust among strangers in internet transactions: Empirical analysis of ebays reputation system. *Working Paper for the NBER workshop on empirical studies of electronic commerce*, 2001.

[8] K. Aberer and Z. Despotovic. Managing trust in a peer-2-peer information system. *In Proceedings of the Ninth International Conference on Information and Knowledge Management* (CIKM 2001), 2001.

[9] A. Jsang. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3):279311, June 2001.

[10] A. Halberstadt L. Mui, M. Mohtashemi. A computational model of trust and reputation. *In Proceedings of the 35th Hawaii International Conference on System Science (HICSS)*, January 7-10, 2002.

[11] A. Josang and R. Ismail. The beta reputation system. *In Proceedings of the 15th Bled Electronic Commerce Conference*, Bled, Slovenia, June 2002.

[12] S. Buchegger and J.-Y. Le Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks). *Proceedings of MobiHoc 2002*, Lausanne, CH, June 2002.

[13] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A Reputation-based Approach for Choosing Reliable Resources in Peer-to-Peer Networks. *In Proc. of the 9th ACM Conference on Computer and Communications Security*, Washington, DC, USA, November 17-21, 2002.

[14] P. Michiardi and R. Molva. Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. *European Wireless Conference*, 2002.

[15] P. Michiardi and R. Molva. CORE: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. *Communication and Multimedia Security*, September, 2002.

[16] N. Li, J. Mitchell, and W. Winsborough. Design of a role-based trust management framework. *In Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, 2002.

[17] S. Bansal and M. Baker. Observation-based Cooperation Enforcement in Ad Hoc Networks. http://arxiv.org/pdf/cs.NI/0307012, July 2003.

[18] M. Carbone, M. Nielsen, and V. Sassone. A formal model for trust in dynamic networks. *BRICS Report* RS-03-4, 2003.

[19] S. Buchegger and J.-Y. Le Boudec. The effect of rumor spreading in reputation systems in mobile ad-hoc networks. *Wiopt03*, Sofia- Antipolis, March 2003.

[20] R. Jurca and B. Faltings. An incentive compatible reputation mechanism. *In Proceedings of the IEEE Conference on E-Commerce*, Newport Beach, CA, USA, June 24-27, 2003.

[21] S. Buchegger and J.-Y. Le Boudec. A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks. *Proceedings of P2PEcon 2004*, Harvard University, Cambridge MA, U.S.A., June 2004.

[22] S. Buchegger, C. Tissieres and J.-Y. Le Boudec. A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks - How Much Can Watchdogs Really Do? *Proceedings of IEEE WMCSA 2004*, English Lake District, UK, December 2004.

[23] S. Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. *In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04)*, October 2004 pp. 66-77.

[24] S. Buchegger and J.-Y. Le Boudec. Self-policing mobile ad-hoc networks by reputation systems. *IEEE Communications Magazine*, July 2005.

[25] J. Mundinger, J.-Y. Le Boudec. Analysis of a Reputation System for Mobile Ad-Hoc Networks with Liars. *In Proceedings of The 3rd International Symposium on Modeling and Optimization*, Trento, Italy, April 2005.

[26] A. Srinivasan, J. Teitelbaum and J. Wu. DRBTS: Distributed Reputation-based Beacon Trust System. *In the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06)*, Indianapolis, USA, 2006.

[27] D. H. McKnight, V. Choudhury, and C. Kacmar. Developing and Validating Trust Measures for e-Commerce: An Integrating Typology. *Information Systems Research*, vol. 13, pp. 334-359, 2002.

[28] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer. Not so different after all: a cross-discipline view of trust. *Academy of Management Review*, vol. 23, pp. 393-404, 1998.

[29] D. Gefen, E. Karahanna, and D. W. Straub. Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, vol. 27, pp. 51-90, 2003.

[30] T.-P. Liang and J.-S. Huang. An empirical study on consumer acceptance of products in electronic markets: a transaction cost model. *Decision Support Systems*, vol. 24, pp. 29-43, 1998.

[31] H. Liang, Y. Xue, K. Laosethakul, and S. J. Lloyd. Information systems and health care: trust, uncertainty, and online prescription filling. *Communications of AIS*, vol. 15, pp. 41-60, 2005.

[32] K. J. Stewart. Trust Transfer on the World Wide Web. *Organization Science*, vol. 14, pp. 5-17, 2003.

[33] P. Dasgupta. Trust as a Commodity. In *Trust*, D. G. Gamretta, Ed. New York: Basil Blackwell, 1988, pp. 49-72.

[34] S. Ba and P. A. Pavlou. Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior. *MIS Quarterly*, vol. 26, pp. 243-268, 2002.

[35] R. J. Lewicki and B. B. Bunker. Trust in Relationships: A Model of Trust Development and Decline. *In Conflict, Cooperation and Justice*, B. B. B. a. J. Z. Rubin, Ed. San Francisco: Jossey-Bass, 1995, pp. 133-173.

[36] D. H. McKnight, L. L. Cummings, and N. L. Chervany. Initial Trust Formation in New Organization Relationships. *Acadamy of Management Review*, vol. 23, pp. 473-490, 1998.

[37] D. Gefen. E-commerce: the role of familiarity and trust. *Omega*, vol. 28, pp. 725-737, 2000.

[38] S. P. Shapiro. The Social Control of Impersonal Trust. *American Journal of Sociology*, vol. 93, pp. 623-658, 1987.

[39] J. Pfeffer and G. R. Salancik. The external control of organizations: a resource dependence perspective. New York: Harper Row, 1978.

[40] S. Ganesan. Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing*, vol. 58, pp. 1-19, 1994.

[41] P. M. Doney and J. P. Cannon. An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing*, vol. 61, pp. 35-51, 1997.

[42] P. R. Nayyar. Information asymmetries: a source of competitive advantage for diversified service firms. *Strategic Management Journal*, vol. 11, pp. 513-519, 1990.

[43] D. P. Mishra, J. B. Heide, and S. G. Cort. Information asymmetry and levels of agency relationships. *Journal of Marketing Research*, vol. 35, pp. 277-295, 1998.

[44] J. Golbeck and J. Hendler. Inferring Trust Relationships in Web-based Social Networks. *ACM Transactions on Internet Technology*, in press.