Trustworthy Wireless Networks: Issues and Applications

(Invited Paper)

Kannan Govindan, Prasant Mohapatra
Department of Computer Science
University of California, Davis, CA 95616
Email: {gkannan, prasant}@cs.ucdavis.edu

Tarek F. Abdelzaher
Department of Computer Science
University of Illinois at Urbana Champaign, Urbana, IL 61801
Email: zaher@cs.uiuc.edu

***Abstract*—Wireless networks are susceptible to various attacks due to their open nature of operations. Existing security mechanisms and systems are rarely robust under attacks, misoperation and internal faults. Most of the solutions are targeted to specific attacks and also works after detecting considerable damage and provides little protection if one or more components are compromised. These approaches are not sufficient for holistic and systemic security. In this paper we analyse a more systematic security approach by exploiting the fundamental relationships among the network components. We explore a concept called trust worthy network where nodes establishes relationships among themselves based on the mutual observations and interactions. These relationships will help to derive the level of security and trust to be possessed on the nodes and the message received from the nodes. We analyse in detail the various issues in constructing the trustworthy networks, impact of various network dynamics on the trust relationships and the applications of trust worthiness in assessing the information quality, to evict the misbehaving nodes and to provide other related security services.**

I. Introduction

In wireless networks generally information is collected from many different sources and processed/relayed by different set of nodes before it reaches the intended destination. In addition mostly the network components are mobile which influences the connectivity among them. In this type of scenario sometimes the nodes will not have much interaction among themselves or prior knowledge due to spare deployment and high dynamism. Establishing a secured communications among these entities is highly challenging and plays a crucial in successful network operations. The highly analysed PKI based security schemes will be hard to manage, implement and easy to break in a highly dynamic heterogeneous networks. As an alternative there are proposal in using physical layer informations to enhance security [1]–[3]. These schemes use physical-layer information or characteristics to detect attacker/malicious nodes and also to provide security services in wireless networks. Due to its availability from the wireless device driver and location distinction property, the received signal strength (RSS) information has been widely used physical layer parameter for attacker/malicious node detection. Physical layer layer security schemes exploit the fact that in a typical wireless multipath environment, the RSS profiles are location specific, that is, they are nearly unique at different locations. When an attacker, who is at a different location than the legitimate user, tries to impersonate the user, the RSS profile would be different from the legitimate one, and then the attack can be detected. Although, these schemes can work well in a static network, they tend to create excessive false alarms in a mobile environment where the RSS profiles are changing over time due to node mobility.

In addition, with the widespread application of networks and development of attack techniques, traditional isolated security prevention can hardly deal with new kinds of attacks. Most of the existing security solutions including the physical layer schemes are mostly a add-on component at the cost of computational resources and they are not exhaustive enough to provide a holistic security systems. They are mostly targeted for specific attack scenarios. The dynamisms and the distributive nature of the mobile adhoc networks call for a holistic mechanisms. The resource constraints and extreme dynamism of the wireless networks deployed for critical missions requires security mechanisms without any additional burden interms of computational complexity or resource management.

Due to this tight requirements there is an increasing interest in exploiting the fundamental relationships among the network nodes to provide security and other related services [4]–[6]. This alternative method will not incur any extra burden as it relies on the natural relationships rather than a added block. The interactions and relationships among the nodes can build a trust among themselves. Trustworthiness turns into the important criteria to evaluate the Quality of Information obtained out of networks. Trust is emerging as an important facet of relationships in wireless networks to ensure a proper operations and successful message transmissions among the network entities.

Whether it is for use in security or accessing the information reliability, or recommender systems, the notion of trust will help a lot extend. The network trust establishment essentially improves the reliability of the information and hence ease the decision making process. However, in high mobile heterogeneous networks like tactical networks establishing the network trust is challenging due to spare deployment, least interactions among the entities and high mobility and dynamism. Trust in itself has many dynamism which will get influenced by the network dynamics. This paper intended to study in detail about the trust establishment in mobile wireless networks and impact of network dynamics on trust dynamics and application of trustworthy networks for practical scenarios. Before we analyse further we need to define trust.

Trust plays a role across many disciplines, including sociology, psychology, economics, political science, history, philos-

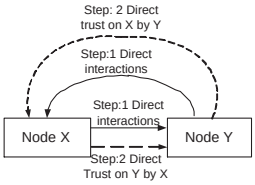

Fig. 1. An example of direct trust evaluation

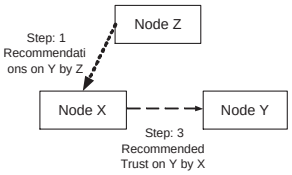

Fig. 2. An example of recommended trust evaluation

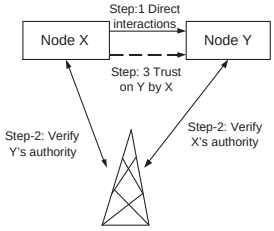

Fig. 3. An example of indirect trust evaluation

ophy, and computer science. As such, work in each discipline has attempted to define the concept [7]. The problem with defining trust is that there are many different types of trust and it means something different to each context. Because the goal of this work is to find a definition that facilitates making computations with trust in wireless networks, we define trust and trust worthy networks with respect to wireless nodes as follows:

DEFINITION 1: **Node Trust**: The trust of a particular node is a subjective assessment by an agent/other peer node on the reliability and accuracy of information received from or traversing through that node in a given situation and given time. The trust value of a particular node reflects any other nodes expectation of its genuineness and provides a sense of influence/control by that particular node over the decision made from the collective information.

DEFINITION 2: **Trust worthy network**: A network where the trust level of every component can be assessed individually or through combination of other nodes.

In the rest of the paper we will analyse in brief about the various trust computing mechanism in Section. II. In Section. III we will discuss about various issues in building a trustworthy networks. Section IV gives some of the dynamics in the trust and impact of various network dynamics on trust is explained in Section V. Section. VI details some of the applications of trustworthy networks with some illustrative examples. Finally Section. VIII concludes the paper.

II. Trust Computations

We can broadly classify the trust calculations/relationships into the following three categories:

- Direct trust
- Recommended trust
- Indirect trust

Direct Trust: Direct Trust is determined by observing the one hop neighbour directly and making sufficient observations, so that their trust relationships are established without reliance on intermediaries. For illustration let us assume nodes are distributed over the region of interest and the communication is multi-hop between nodes. Nodes can misbehave based on application for which they are deployed. For instance, in the case of event monitoring the nodes can report arbitrary false information or in the case of multi-hop cellular networks nodes can misbehave by dropping packets. Let us assume every node makes observation about the neighbor nodes behavior and make a 'opinion' about its neighbors. Nodes follow the process of overhearing sensor readings of nearby nodes and then compare the readings with their own local sensor readings. If the remote sensor readings are correlated closely enough with the local sensor readings (they are within a threshold set by decaying the correlation of values based on the distance between the sensor ranges), then the remote sensor reading is considered to be valid. For instance let us assume that node n observes a event and measures I_n as the intensity of the event and a observes the intensity of the event as I_a as reports it. Now the direct trust of a observed by n is

$$T(n,a) = \frac{I_n - I_a}{I_n} \quad (1)$$

Recommended Trust: Recommended Trust is determined from the recommendation third parties give about a particular node. Recommended trust can be of two types: Pull-aggregate based and Push-aggregate based schemes. In the Pull-aggregate based scheme a trust requesting node will need to find the trust information provider on the target node, and pull the trust information and aggregate different trust value from different providers. In the Push-aggregate based trust propagation process each participant node in the network who has evaluated the trust of the target node and also willing to share the evaluated trust information, will push its evaluated trust value on target node to other participants in the network, any participant can collect its interested trust information, and aggregate them from different propagation path.

Indirect Trust: Indirect Trust is obtained when communicating entities verify the validity of each others based on the key/authorization given by the centralized server. Indirect trust also involves interactions like direct trust methods however here the interactions requires authentication and verifications from the authentication server. In a way indirect trust is a combination of both direct trust and recommended trust as it requires recommendation from the central server and also the direct interactions among the nodes.

III. Issues in building the trusted networks

Building a trust worthy networks involves the following major issues. The complexity is essentially depends on which method is used in determining the trust. Though the following analysis is not a complete set, these are very commonly encountered issues:

Computational resources: In trust evaluations every node has

to have memory to store past interactions history, the recommendations from other nodes and also the present interactions details. There will also be a detailed mathematical calculations to determine the trust value based on all these stored data depending on which method one chooses to determine the trust value. In addition incase of recommended trust the communication bandwidth in transporting the trust informations from one node to distance node also a resource expensive task. Furthermore, there will be computation involved interms of aggregating the values when there are multiple recommendations and multiple version of the trust measurements.

Infrastructural Complexity: The infrastructure required in the case of indirect trust evaluation is a centralised trust authority which monitors every node. Every node requests the centralised authority to verify the authenticity of the fellow node before believing in the behaviour.

Scalability: Scalability could be a issue in building trustworthy networks. Direct interactions and meeting face-to-face point might boost the establishment of trust relationships, but only in a small network size. For instance, in a large network environment, nodes might need to travel a long distance to reach the meeting point. Besides, in the case of indirect trust evaluation a centralized authority (CA) also might be required to ensure security at the meeting point, which could easily be exploited by attackers if not taken seriously.

Trust mechanisms have to designed with the resource constraints and the other above mentioned challeneges into considerations. Though we cannot address all the issues completely its important to have a comprehensive solutions by taking take of critical challenges.

IV. Trust Dynamics and Properties

A. Trust dynamics

The evolution of trust over time is called the dynamics of trust. Trust is a dynamic phenomenon. Trust changes with experience, with the modification of the different sources it is based on (e.g., environment, mobility etc), with the state of the trusting node and so on. The trust dynamics can be characterized by the following phenomenon: Trust propagation, prediction and aggregation. From the propagation of trust we can determine the change in trust values of nodes without directly interacting. Aggregation of trust helps to aggregate the trust value propagated through multiple paths so that a single aggregated decision can be made on the dynamic change of trust. Trust prediction helps to determine the future change in the trust value. In the following we give brief explanation about these dynamics.

Aggregation:
Trust aggregation problem consists of aggregating n-tuples of observed trust values all belonging to a given set, into a single trust of the same set. In this setting, an trust aggregation operator is simply a function, which assigns a real number trust value y to any n-tuple observed trust value $(x_1,\ x_2, \ldots, x_n)$ of real numbers

$$y = Aggre(x_1,\ x_2, \ldots, x_n) \tag{2}$$

Trust Propagation:
Once the trust is computed by any of the node(s), the resources spent on computations by other nodes can be reduced if the computed trust of a node gets propagated in the network. If a node A get to know the trust value of node X though node B, C, . . ., then node A can actually avoid the explicit trust computation on node X. This is particularly important in infrastructureless distributed systems.When trust value is computed, it includes information transition and exchange from one node to another. Therefore, the propagation of trust is highly correlated with the computation of trust.

Trust Prediction:
Trust prediction is method of predicting potentially unknown trust between nodes using the present and past behaviour of nodes and also the recommendations received from other nodes.

Trust dynamics help highly to establish the trust with minimal computational resources. Trust dynamics especially trust propagation and prediction can help to avoid the risks of having insecured communications by predicting the future behaviour of the nodes. By wisely combining the trust dynamics with the trust computations we can achieve maximum performance improvement in the network.

B. Trust properties

In this section, we present several properties that are closely related to computation [8].

Trust Transitivity:
One of the primary properties of trust that is necessary for computation is transitivity. Trust is not perfectly transitive in the mathematical sense; that is, if Alice highly trusts Bob, and Bob highly trusts Jack, it does not always and exactly follow that Alice will highly trust Jack. There will always be a degradation/enhancement by the individual or group of nodes on the propagation path while propagating the trust.

Trust composability:
The trust values of each neighbor, and their recommendations about a particular node should all be composed together and should all lead to a single final aggregated trust which is also belong to the same set as the original trust information. Different compose/aggregation function can be used to aggregate the trust information depending on the situations and the kind of trust informations. The aggregation operator should satisfy the conditions set for the aggregation [9].

Personalization and Asymmetry
One property of trust that is important in social networks, and which has been frequently overlooked in the past, is the personalization of trust. Trust is inherently a personal opinion. Two nodes often have very different opinions about the trustworthiness of the same target node. In addition trust on node A by node B not necessarily same as the trust on node B by node A. When we determine the trust of nodes and build a trust worthy network we need to take care of these properties.

V. Impact of network dynamics on trust dynamics

In this section we analyse impact of various network dynamics on the trust and behaviour of the wireless network.

Network behavior we mean the information delivery capability of the network in terms of quality of information. First we will analyze in detail about the various network dynamics that can have considerable impact on the trust and behavior in the network and then analyses the impact of each parameters in detail. Following are the some of the widely considered network dynamics:

Heterogeneity:

Most of the present day wireless networks are collaborative networks and involves nodes of many varieties, different types, capabilities, specifications and different nations. These heterogeneity among the nodes brings challenges in constructing unified trust mechanisms and a global trustworthy network.

Mobility:

Present days networks are highly mobile for example V2V networks, tactical networks and mobile adhoc networks. There may be a mobility of different types among the nodes in the networks: low mobility (human walking) or high mobility (mobility of sensors mounted on vehicle). There may be multiple, mobile command centers and/or combinations of static and mobile centralised authorities. These combination of mobility makes trust building complicated as the node association changes due to mobility and hence the time of observation. These things can hammer the trust building and establishments.

Link Stability and Topology:

The network composition may significantly change with time in an unpredictable manner, in various ways: failures occur, nodes may periodically fall asleep to save power, nodes may be added incrementally during the network evolution, or nodes may die off due to energy draining. Topology of the network can change due to these network phenomenons. The neighborhood of node and hence the social relationships change due to change in the topology. These change in topology can have adverse effect on the trust relationships.

Environmental Factors:

Physical obstacles of various shapes, size and harshness in the deployment territory (strips, convex, concave) and types (physical/communication, deterministic/stochastic) further obstruct the network links. The environment may be hostile and even malicious, i.e., security attacks may threaten the individual devices and the network, introducing adversarial dynamicity. Even the performance goals of a given network in operation may change with time because of application-dependence.

Social relationships:

In heterogeneous network social relationships among a set of nodes is common. Nodes can form subgroups based on the previous relationships with the good/bad intention in mind. Social relationships among the nodes can impact trust. It can negatively impact the trust rating or positively too. For instance, set of nodes can form a sub group and give a very positive rating about each other to enhance the trust ratings of each other. This way the social relationships among nodes help them to play a cooperative game to enhance each others trust. Therefore, the information flows through this network need not to be delivered to the right address or it may be delivered with the altered content. However, the trust of the information may still be very high due to the cooperative gaming of nodes. In positive sense, the social relationships among the node can help them to find the misbehavioural or untrustworthy nodes in a cooperative way. Therefore, the information can be diverted from these misbehaviourals nodes while routing or the information originated from these nodes can be ignored or given less weightage.

Despite these high dynamics, the network should operate in a trustworthy manner. Impacts of these dynamics on the trust and network behavior have to be taken care before we design the networks.

Trust computations in a high dynamic networks:

Trust and network dynamics are closely interrelated and affect one another. For example a node can change the association with the neighbor when it finds the trust level of the neighbor drops down. That means the dynamics of the links changes due to trust of the nodes. On the other hand, a node will not trust/rely much on its neighbor who is continuously moving. That is, the dynamics affects the trustworthy factors. The trust relationship is function of the level of dynamisms expected from the neighbors and vice versa. It is important to start with some assumption on dynamics modelling. Having the notion of network dynamisms in mind we can determine the relationship between network dynamics and trust. Once a trustworthiness of the node is found, it can be propagated to the network as recommendations so that trust of nodes which are more than one hop away can be found at the quickest time using recommendation trust calculations. In a social network, a key factor influencing the behavior and decisions of entities is their level of interpersonal trust and propagation of trust amongst entities in these vast networks. For example in real life, individuals and businesses give referrals (trust propagation) and rely enormously on referrals to determine with whom to interact. In a similar way we work on modelling the networks security behavior based on trust and also work on trust propagations. Network dynamisms in particular mobility and heterogeneity can be exploited as a method of propagating trust in the networks. Even combination of many of the dynamisms property can be exploited to establish trust in a quickest time possible in the networks. Different dynamics affects the trust and its establishment in the network. This will eventually affects the information delivery and hence the network behaviors. The positive impact of dynamics on the trust will enhance the quality of information and hence the network behavior. On the other hand the negative impacts make network behave poorly. The impact of network dynamics on the various dynamics is shown in Table. I

VI. Application of trust worthy networks

Trust can be used in many fields in wireless networks for the successful network operations. We discuss the following three applications with illustrative examples.

A. Quality of information estimation

In modern days network, information transmissions and sharing are the essential activities. Information from differ-

TABLE I
INFLUENCE OF VARIOUS NETWORK DYNAMICS ON THE TRUST DYNAMICS

Network Dynamics	Trust Dynamics		
	Trust Propagation	Trust Aggregation	Trust Prediction
Mobility	Mobility helps to propagate trust naturally [10]. The more mobility the more quicker will be the propagation of trust.	Mobility improves the aggregation too. There are more chances of collecting more trust data for aggregation as the mobility increases.	Mobility may weaken the trust prediction as it will be difficult to track the behaviour as the nodes move away.
Network density	More dense the network is, more faster will be the trust propagation as the density links make the information flow easier.	Aggregation also improves with the node density as more data will be available for aggregation when the network density increases hence the error in aggregation will be minimal.	More dense the network more samples available for prediction hence the prediction improves with the network density.
Link breakages	Link breakage makes the trust propagation worse. More volatile the link more severe its effect on propagating the trust information.	Link breakage affects the trust aggregation and the error is aggregation may manifest due to link breakages.	Link breakage affects the trust prediction too. Because, when the link breaks it is hard to predict the behaviour whether it is because of link volatility or due to node's behaviour.

ent sources makes it possible to extract more accurate and complete knowledge and thus support more informed decision making. However, high quality and trustworthiness of received information is crucial to the decision makers so that any bias on the decision can be avoided. For the information to be trustworthy it has to be received from trustworthy sources. When some information is derived from various data items gathered from multiple sources, it is possible that no data value satisfies an evaluators requirement with regard to information quality, if they are evaluated separately. According to the principle of object trust combination, if the final values of an object calculated by using significantly different methods are similar, then the evaluator places higher level of trust in the results [11]. Intuitively, different versions of the same event that are calculated in different ways but have similar values provides "multiple-proofs" towards their correctness.

Now let us assume a information is generated by collecting data items from different sources about the same event. Further assume that every data item is embedded with the provenance details of the nodes who performed operations on it. Now once the data items are gathered at the receiver by correlating the data items from different paths we can determine the trust levels on the data items and also the nodes who performed operations on it [12]. This data items trustworthiness will determine the quality of information generated and hence eventually help the decision maker to make the optimum decision.

B. Malicious node detection

Since the nodes are highly dynamic and heterogeneous in mobile wireless networks it is common that nodes tend to misbehave purposely or unknowingly. It is critical to detect and isolate the compromised nodes in order to avoid being misled by the falsified information injected by the adversary through compromised nodes. However, it is challenging to secure the heterogeneous networks efficiently because of the poor scalability and high communication overhead. However, trust evaluation schemes can be used as a natural way to detect malicious nodes in wireless networks [13]. Let us assume every node keep monitors the behaviour of the adjacent nodes and report the adjacent node as malicious node whenever the trust level drops below certain level. Now by correlating the reports received from many nodes on a given particular node, every node can determine an aggregated trust and can restrict the communication to the node whose trust is below certain level. The low trustworthy node will eventually get isolated and removed from the network. The malicious node eviction can be carried out by utilizing clustered topology which reduces the communication over head.

C. Secured communications

Trusted network can be used in other security services like authentication and access control. For instance a trust based access control and authentication for peer-to-peer network is proposed in [14]. The proposed authentication procedure works as follows. First, the client sends an authentication request, containing its ID and public key together with a secret encrypted by the hosts public key, to the host. Upon receiving the request, the host checks in its database to see if the client has previously contacted it. If so, there will be some existing trust information. If the client has not previously contacted the host, then the host will create a database entry for it. The host then carries out an authentication protocol based on the trust history and credentials of the requester.

VII. RESEARCH SCOPE

It is clear that trustworthy networks and computing provide security benefits, if a detailed algorithm is worked out to take advantage of it. But trusted computing has been received with cautious so far and remain as a debated area of research. Some of the issues are yet to be addressed, but much of them are appropriate. Trusted computing systems fundamentally alter trust relationships. There are many concerns growing in this area of research. Legitimate concerns about trusted computing are not limited to one area, such as individual's privacy but also to the level of accuracy, computational requirements etc.

Though the following set is not complete, we can clearly identify these important issues which need research focus.

A. Trust building and convergence in a dynamic networks

In a high dynamic networks the network connection may get lost often due to network dynamics. In addition the communication itself may get disturbed highly due to wireless media. Hence the interactions based trust may not be accurate and nodes may get victimized for no faults. The interactions

itself may not happen so often when the network density is low and the nodes keep moving. In such a scenario the secondary recommendations from other nodes can help set up the recommended trust. However, the main issue is the convergence time. How long a node has to wait or how much samples are good enough to make a right decision about the trustworthiness same time avoid enough damage from the malicious node. These relationships have to be worked out in detail.

B. Trust computations in cooperative and non-cooperative environments

Trust computation in a distributed network restricted to only local interactions and observations by a individual nodes. Each node, as an autonomous agent, makes the decision on trust evaluation individually. The decision is based on information it has obtained by itself or from its neighbors. Those aspects are analogous to situations in statistical mechanics of complex systems with game theoretic interactions. In this network if there is a propagation of trust, then the network may get attacked easily. For instance a set of malicious nodes can form a group and give a positive trust value on each other and play a cooperative game. Trust evaluation under a cooperative gaming remains a open problem. Even the primitive case of it, i.e., the trust evaluation in a non cooperative game is unsolved. In a non cooperative game every node behaves very well in a non critical situations to improve its trust rating and misbehave once in a while to cause considerable damage and still remain undetected.

C. Exploitation of Trustworthy networks to provide security services

The main security services expected out of networks are confidentiality, integrity and availability. Mostly these security services are achieved though a application layer algorithms. These algorithms are targeted for specific scenario and applications and mostly requires complex mechanisms to manage. The data delivery capabilities and security properties of the network directly impact the level of trust a recipient palaces on the information received. As an example it is possible that a piece of information cannot be fully trusted unless its source and the path over which it is received are authenticated. If authentication services are not available one must decide whether to have the untrusted information or none at all. If obtaining the information with utmost level of trust requires degrading the delivery of the information (i.e., increasing its latency), one has to determine whether this is the right trade-off. On the other hand it is possible that due to the latency incurred the information may become invalid by the time it is received; in such a case the trust in the information is again reduced. Further research is required to characterize these metrics through modelling efforts and to determine the degree to which security properties influence the network trust.

VIII. Conclusion

Trust and its management are exciting fields of research. The rich literature growing around trust as well as the implementation of trust systems in commercial application, give a strong indication that this is an important area of research. Trust as a concept has wide variety of adaptations and applications, which causes divergence in trust management terminology. The goal of this paper is to provide wireless network designers with multiple perspectives on the concept of trust, an understanding of the properties that should be considered in developing a trust metric, and insights on how a trust can be customized to meet the requirements and goals of the targeted system. The trust metrics can be utilized to construct a trust worthy networks which can be used in many applications and security services.

Acknowledgement

This work was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-09-2-0053. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official polices, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copy right notation here on.

References

[1] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the physical layer for wireless authentication," in *IEEE International Conference on Communications ICC-07*, pp. 4646–4651.

[2] Y. Sheng, K. Tan, G. Chen, D. Kotz and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," in *IEEE INFOCOM 2008*, pp. 2441–2449.

[3] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571–2579, 2008.

[4] P. Lamsal, "Understanding trust and security," in *Technical report, University of Helsinki, Finland*, 2001.

[5] G. M. Coates, K. M. Hopkinson, S. R. Graham and S. H. Kurkowski, "A Trust System Architecture for SCADA Network Security," *IEEE Trans. Power Delivery*, pp. 158–169.

[6] P. Albers and O. Camp and J. Percher and B. Jouga and R. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," in *In Proceedings of the First International Workshop on Wireless Information Systems WIS-02*, pp. 1–12, 2002.

[7] D. H. Mcknight and N. L. Chervany, "The Meanings of Trust: University of Minnesota, Technical reports." http://misrc.umn.edu/wpaper/WorkingPapers/9604.pdf, 1996.

[8] J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," in *Securecomm and Workshops-Security and Privacy for Emerging Areas in Communications Networks*, pp. 1–7, 2006.

[9] M. Detyniecki, "Mathematical aggregation operators and their application to video querying," 2000.

[10] F. Li and J. Wu, "Mobility Reduces Uncertainty in MANETs, in IEEE International Conference on Computer Communications," in *INFOCOM07*.

[11] Y. Zuo and B. Panda, "Information trustworthiness evaluation based on trust combination," in *SAC '06: Proceedings of the 2006 ACM symposium on Applied computing*, pp. 1880–1885, 2006.

[12] X. Wang, K. Govindan, P. Mohapatra, "Provenance Based Information Trustworthiness Evaluation in Multi-hop Networks," in *Globecom, 2010*.

[13] I. M. Atakli, H. Hu, Y. Chen, W. S. Ku and Z. Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation," in *SpringSim '08: Proceedings of the 2008 Spring simulation multiconference*, pp. 836–843, 2008.

[14] H. Tran, M. Hitchens, V. Varadharajan and P. Watters in *The Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 2005.