I.J. Computer Network and Information Security, **2014, 10, 64-71**
Published Online September 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.10.08

Trust Metric based Soft Security in Mobile Pervasive Environment

Madhu Sharma Gaur
Ph.D. Scholar GEU, Dehradun, Asst. Prof., G. L. Bajaj Inst. of Tech & Mgmt. Greater Noida,
madhu14nov@gmail.com

Dr. Bhaskar Pant
Asst. Prof, Deptt of IT, GEU Dehradun,
pantbhaskar2@gmail.com

Abstract—In the decentralized and highly dynamic environment like Mobile Pervasive Environments (MPE) trust and security measurement are two major challenging issues for community researchers. So far primarily many of architectural frameworks and models developed and being used. In the vision of pervasive computing where mobile applications are growing immensely with the potential of low cost, high performance, and user centric solutions. This paradigm is highly dynamic and heterogeneous and brings along trust and security challenges regarding vulnerabilities and threats due to inherent open connectivity. Despite advances in the technology, there is still a lack of methods to measure the security and level of trust and framework for the assessment and calculation of the degree of the trustworthiness. In this paper, we explore security and trust metrics concerns requirement and challenges to decide the trust computations metric parameters for a self-adaptive self-monitoring trust based security assurance in mobile pervasive environment. The objective is to identify the trust parameters while routing and determine the node behavior for soft security trust metric. In winding up, we put our efforts to set up security assurance model to deal with attacks and vulnerabilities requirements of system under exploration.

Index Terms—Metrics, Mobile Pervasive Environment (MPE), Security Assurance, Trust Metrics.

I. Introduction

In the decentralized and highly dynamic environment like Mobile Pervasive Environments (MPE) trust and security measurement are two major challenging issues where small, powerful and resource-restricted devices are communicating seamlessly. Such environment does not have fixed infrastructure and centralized access control thus needs to be self-adaptive and self-organizing. There are mobile hosts which can link to the network on the air and can be deployed rapidly with the potential option for dynamic security. Furthermore, the self-adaptive self-organizing communication can survive better in critical situation like war, terrorism or natural disaster scenarios compared to fixed infrastructures. Our approach focus on trust based soft security with the assumption that strength of security assurance can be enhanced by identifying strong and weak trust parameters as trust metric. In this paper, we explore security and trust metrics concerns requirement and challenges to decide the trust computations. The objective is to identify the trust parameters while routing and determine the node behavior. In winding up, we put our efforts to set up general security assurance model based on trust and security vulnerabilities requirements, behavior modeling evidence collection, and the assessment security level of the system under exploration. The major contributions of this work are:

- Recognizing security concerns and requirements,
- Trust management.
- Identification of sophisticated information security metric for Mobile pervasive environment,
- Defining trust based soft security assurance metric
- Performance Evaluation

The rest of the paper is organized as Section II Literature Review and section III describes the MPE security concerns, requirements and metrics. In the section IV Trust Definition and Trust Management V. metrics VI- Proposes Approach and finally in section VII Conclusion and future scope.

II. Litrature Review

The security objective typically consists of security requirements like integrity, privacy, confidentiality, availability as per specifications or standards. The probability of quantify security and developing security metrics, one has to be aware about the facts that the metric simplifies a complex socio-technical situation. Security metrics are. Pioneering work on trust management [1] had as its goal separation of security and trust [3]. The benefit of the separation is allowing individual systems to have different trust policies, separate from the common, global authentication and security system. Rasmusson and Janssen [11] identified two approaches to security: hard security and soft security. Hard security is used to traditional security mechanisms like authentication, authorization, access control. It usually protects resources from attacks intruders or malicious user's unauthorized access such as overwhelming information (denial-of-service attacks) or false information (phishing). Hard security scheme cannot help in detecting/preventing behaviors continuously varying. Binary type of solution will not be also effective. As well as reliability and trustworthiness of the information received from nodes, quality of information assessment and providing various levels of access control cannot be done efficiently through hard security. Thus Soft security is required in such scenarios. It relies on trust management systems, reputation systems, and other "society" of artifact. In this proposed work we present a trust based soft security scheme. Trust management systems, such as PolicyMaker [1], and REFEREE [4] began by automating authentication and authorization decisions with the help of varying sets of credentials. Blaze et al. [1] defined trust management as "a unified approach to specifying and interpreting security policies, credentials, relationships which allow direct authorization of security-critical actions. Cho and Swami [3] explain that trust management includes trust establishment (i.e., collecting appropriate trust evidences, trust generation, trust distribution, trust discovery, and evaluation of trust evidence), trust updates, and trust revocation and also provide summary of existing trust management schemes listing the schemes by name, methodology of collecting trust evidence, attacks targeted, performance metrics used, and other notable characteristics. The discussion of trust in literature is generally considered a domain-crossing subject with domain specific view and determination of the concept. Still, the implication of trust can be inherited by differing domains with many trust facets like Trust as risk factor: The definition given by Morton Deutsch [7] is more widely accepted than many, and states that trusting behavior occurs when an individual (node) perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the good or bad result is contingent on the actions of another person.

III. Security Concerns and Requirement

A. *Security Concerns:*

Well-known general security dimensions include confidentiality, integrity, availability, non-repudiation and authenticity. Quality attributes like usability, robustness, interoperability are other important concern issues. In general, the existing research has noted that traditional security solutions, such as public key infrastructures, or authentication mechanisms, are potential solutions also for ad hoc networks, but in many cases they are not sufficient by themselves. With mobility pervasive environment raised new security Challenges and the ultimate goal is to provide secured and trusted services with the objective of confidentiality, integrity, availability, authentication, authorization and non-repudiation, at desired security level. The nature of the basic mechanisms of the mobile communication paradigm causes a pervasive environment to be vulnerable due to:

Decentralized Administration: There is no central administration, control or prior contact is assumed;

Resource Constrained: In MPE dissimilar small-sized, resource-restricted (limited memory, power, bandwidth) devices or nodes communicate seamlessly. Sleep or standby modes are used to conserve energy, during which they may not be reachable. Sleep deprivation torture is used by attackers. The heterogeneity of node capabilities can result in asymmetric links;

Mobility: It is the phenomenon moving while keeping device communication. Mobility in networks can be considered on different granularity levels, depending on the access point, access point region, location area, domain, or network.

Lack of Mechanisms of Identity control: Devices spontaneously connected and due to lack of central administration the big challenges in the identity management of non-operator-controlled PME.

Co-operation: Algorithms in pervasive environment are assumed to be self-adaptive, self–organizing and co-operative. Other notable security concerns for MPE are

- The communication nature is momentary and ad-hoc and Complicated to manage the uncertainty.
- A devices must be able to review about its trusted peers
- Authentication, Privacy Availability
- Trust management
- Decentralized administration and bigger physical attack surface with multi spot of failure
- Devices have no prior knowledge of about peer and communicating un-known by the user.
- Implement mechanism with Recourse Restriction

B. *Security Requirement:*

Security requirement is an expression of a high-level organizational security policy with the detailed requirements of a specific system [4]. If we want to measure the security behavior of an entity in the system, we can compare it with the explicit security requirements, which act as a "measuring rod". Since security is clearly a system-level problem, one cannot accurately determine the security requirements outside the context and environment of the system. On all the security dimensions with quality attributes should be addressed in the definition of security requirements. The functional part of Common Criteria includes:

- General-level requirement lists and can be used as guidance.
- Building security requirements is often a process of making trade-off decisions between high security, high usability and low cost.
- The actual requirements and role of the security dimensions heavily depend on the system itself and

its context and use scenarios.

- The requirements should also represent sufficient system design and security countermeasure design information.

Unluckily, widely accepted and succinct collections of security requirements are not available and directly implacable for mobile pervasive devices. A compositional approach is used to define security metrics with the following iterative, steps:

- Security Metrics Objectives: The security objectives are defined based on the knowledge of the secure environment, assumptions and threats. Among other things, they should determine the required security level by;
- Identification of Measurable Components: Exploring the security measurable components.
- Finding components inter-dependency: Find dependencies between different components and if required refining and redefining will be done independently.
- The composition of integrated security level information: Finally combining the depends mainly on the method of measurement. The composition can be used for both quantitative and qualitative security metrics.

IV. Trust Definition And Trust Management

Trust is another important aspect of mobile and heterogeneous networks that enables the communicating entities to deal with uncertainty and uncontrollability. Trust computations and management are highly challenging issues due to computational complexity constraints and the independent movement of component nodes. There are numerous definitions given to trust in literature reflected by reliability, utility, availability, reputation, risk, confidence, quality of services and other concepts. Nevertheless, none of these concepts can accurately describe the definition of trust. This is because trust is an abstract concept, which combines many complicated factors [5]. As per standard definition of trust "it is a measure of subjective belief that one person or party uses to assess the probability another will perform a favorable action before the opportunity presents itself to monitor whether that activity has occurred". In the literature Trsut has been defind in different ways like - Trust as belief: Trust is an individual's belief and willingness to act on the basis of the words, actions, and decisions of another. Trust as subjective probability: Trust is a particular level of subjective probability with a particular action for a specified time with given context. Trust as transitivity relationship: Trust is a weighted binary relation between two members of a network. As an example, consider a network of intelligence gathering agents, organized in a hierarchical manner.

Types of Trust: A few different classifications of trust help understanding its meaning and scope. In the first classification, two types of trust are distinguished: subjective trust and decision trust.

Subjective trust is "the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends."

Yet another popular classification creates a dichotomy of direct and indirect trust.

Direct trust is established through observations on whether the previous interactions between the subject and the agent 2 the original name "reliability trust" has been changed by us since, in our opinion, it abuses the term "reliability" that has a very precise technical meaning.

Recommendation trust—often determined by checking consistency between one's observations and received recommendations, or among multiple received recommendations is a subset of direct trust.

Indirect trust is due to the fact that trust can be transitive through third parties.

Components of Trust: Most advanced trust management systems use reputation and vide a reputation-based trust management framework presented by Conner et al. [Hard trust solutions build up trust through structural and objective regulations, standards, as well as widely accepted rules, mechanisms and sound technologies. In contrast, soft trust solutions provide trust based on trust evaluation according to subjective trust standards, facts from previous experiences and history. In particular, hard trust can verify functionalities of soft trust solutions, and soft trust solutions can help in selecting suitable and complementary hard trust solutions (and determine when they should be applied).

Trust Management: The perception of trust management for network security was first conceptualized with PolicyMaker [1]; a distributed trust management framework that first investigate into the "trust management problem", moving the idea of trust security away from simple third party certificating. The framework allows flexibility to support trust relationships and localized control through public keys to access control without hard security authentication. This carried the idea that the subjective value of trust could be realized by each party/node within the network, rather than just on a global scale.

VI. Security and Trust Measurement and Metrics

It is ready to le nd a hand to become aware of the two terms i.e. measurements and metrics where:

Measurements: provide single-point in- time views of specific, discrete factors and

Metrics: are derived by comparing two or more measurements taken over time with a predetermined baseline

Payne [9] remarks that truly useful security metrics indicate the degree to which security goals, such as data confidentiality, are being met.

Security metrics: Federal Information Processing Standards (FIPS) Publication 1999 presents Security metrics as a mechanism for investigating confidentiality, integrity and availability separately, emphasizing the assessment of potential impact.

- Security metrics are decision support practice for security risk assessment and management (mitigating, canceling or neglecting)
- Security metrics are the assessment or measurement techniques against the security risks.
- Security metrics can be obtained at different levels of the system as well as comprehensive metrics can be aggregated and rolled up to increasingly upper levels.
- Security metrics can be quantitative or qualitative, objective or subjective, static or dynamic, absolute or relative, or direct or indirect.

Payne [9] states that security metrics can distinguishes the effectiveness of a particular component of a security program, indicate the security of a specific system. A technical security metrics model consists of three components:

- The object being measured,
- The security objectives, i.e. the reference the object is being measured against, and
- The method of measurement.

Information Distribution*:* Critical information distribution in a MPE means the network, meta-data and storage information is identified in

- Mobile unit Context awareness,
- Routing information, and
- Packet forwarding information
- Trust information (e.g. keys, certificates, signatures),
- User-Centric acceptance

Trust Metrics: To compute the trust level on nodes, it is imperative to recognize trust characteristics and metrics for trust computations. Trust Metrics measures it’s correctness by performing cross-validation to make sure that our models are tuned for utmost correctness without being statistically over-fitted. We double-check performance on “proposed sets” as well as pertaining continuing “human” quality assurance for an algorithm. Trust Metrics combines state-of-the-art statistical modeling techniques with proprietary facts and unique grading. This combination enables the Trust Metrics to formulate unique algorithms that effectively and accurately identify many different classifications for concept.

Trust Metrics measures it’s accuracy by performing cross-validation to ensure that our models are tuned for maximum accuracy without being statistically over-fitted. We double-check performance on “holdout sets” as well as applying ongoing “human” quality assurance for every algorithm. Trust has been evaluated using different metrics and different ways. In the literature, there are following trust metrics categories:

Trust scale: Some schemes use continuous or discrete values to measure the level of trust. trust is described by a continuous value in [0, 1] and Threshold based approaches are also used to measure the trust

Trust facets: Confidence value c in the interval [0, 1] and a trust value in the interval [0, 1] together denote the trustworthiness of a node. The trust value (T) represents the observed trust value and confidence value (C) represents the level of confidence a node has on the observed trust value.

VII. Proposed Approach

Security issues have strong influence on the trusted usability of mobile pervasive devices which depends upon the level of security awareness and secured service confirmation. So a security architecture based on trust is required to handle soft security and privacy problems. In future networks and pervasive computing environments, people will be surrounded by zillions of computing devices of all kinds, sizes, and propensity. Fundamentally changed reality demands new approaches to security (authentication and privacy) that socially based paradigms, such as trust-based approaches, can enhance future networks as well as pervasive computing.

Trust based soft security: A malicious node detection mechanism based on trust computations for wireless adhoc network is proposed in [6] where a trust authority collects the grievance from users about the neighbor’s malicious activities and trust authority integrates its direct observations on malicious node with the reported complaints from authenticated devices Authenticated nodes aggregate the global trust vector received from the trust agent with their local trust vector to decide what level of trust to assign to a device. Malicious nodes will be detected whenever this trust level drops below a certain threshold.

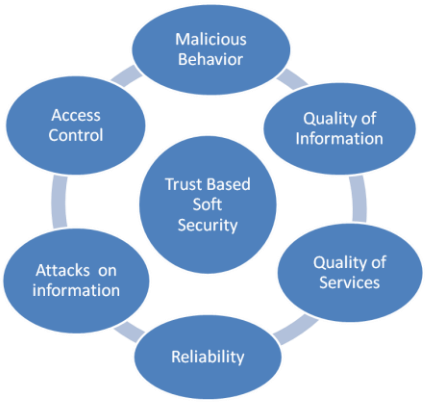

Fig.1 Trust based Soft Security Components

A trust-based misbehavior detection and secure routing model known as Secure MANET Routing with Trust Intrigue (SMRTI) is proposed in [12]. A similar approach of hybrid trust evaluation as in [6] is followed here. SMRTI applies the trust prediction strategy and then decide whether to forward or not. Trust management cannot be seen as a complete replacement for cryptography, rather a supplement to it. Cryptography and trust managements can work together to provide holistic security solution in MANET. While the literature review [6],[11],[14] and [15] we found various soft security services such as routing, malicious node detection, quality of information assessment, node reliability/trustworthiness using trust based approach.

System Model and Assumptions: A pervasive environment is characterized by a richness of contexts in which users, devices and agents are mobile. The availability of contextual data provided by sensors can be used to extract behavior patterns of the mobile entities (users, devices, agents). Context awareness can bring a valuable help to understand the relation between users, devices and environments. Owing to the big range and variety of sensors deployed, the pervasive space can provide a very rich and valuable information set which can be used to derive. Most important contribution of proposed work is the utilization of resulting the trust to enhance security assurance in existing routing protocols. We rely on existing methodologies for obtain trust and certain assumptions about the routing protocol and lower layers.

We consider impulsive behavior appropriate for trust based methods. Primary attackers we consider are of the form Active-0-x, i.e.: the attacker controls n_x external nodes. Such Pretender, though apparently unsophisticated, cannot be prevented by cryptographic methods and needs some other trust based methods. The objective of such an Pretender is to become a part of maximum number of routes, using minimum resources. This enables the Pretender to mount pervasive attacks that can disgrace the performance of a quite big area of the network (large no of nodes). Let’s assume a scenario where an Pretender can selectively drop packets, or misuse the resources of under attack nodes by causing significant action through it. We may also consider a subset of adversaries of form Active-y-x, i.e.: the attacker controls ni internal nodes of the network and nx total nodes. For such Pretenders, we can consider such actions that are restricted to selfish behavior i.e. selectively forwarding traffic, or relaying large amounts of traffic to increase the relay payoff. Such attackers may also launch attacks by readily participating in the control phase and selectively forwarding in the data transmission phase. Such behavioral manipulations to the protocol cannot be effectively dealt with using cryptographic methods. Thus they rely on trust based mechanisms.

A. Trust based soft security metric factors:

In our proposed approach we consider soft security metric factors affecting the reliability estimation based on the trust of a link or a communicating node as delay decisions about a packet are made at the receiving node. We assume that the receiver has methods to evaluate the trust in the link over which the packet was received and the trust value associated with the behavior of the sending node. Different metrics may be representative of trust at different layers of the communication stack. Such metrics can typically be obtained independently from one another. In case of presence of several mechanisms of obtaining trust, we can compute the overall trust as a weighted combination of different values, with the weights depending on the source of the value. This allows us to adjust the significance of different type of trust applicable to the deployment scenario. As an example, assume we have available the link trusts $t_1,t_2 \in [0,1]$ and node Trust $t_3 \in [0,1]$ We can consider simple linear combination

$$T = C1\ t1 + C2\ t2, + C3\ t3 \qquad (1)$$

Where C_i is the cost of ith metric. Suppose there is an environment with a strong encryption, the apprehension for eavesdropping will be low and similarly where we have strong error correcting code for blocks of data, than we can bear rational no packet loss. Thus lower the cost to node trust, obtained from behavioral analysis. In this approach control plane for on-demand protocols, by modifying the flow of route discovery packets based on the trust value of nodes and links. Two functions f1(t) and f2(t) such that f1, f1 : [0, 1] ->D, to represent trust based delay.

Assume t2 [0, 1] denotes the combined trust evaluation of link over which the packet was received and the node from which it was received. We modify the behavior of a node receiving the route discovery packet as follows

- Upon receiving the route discovery packet for a constant time f1(t) prior to broadcasting it.
- In case the node senses a packet collision or a busy channel, instead of a standard binary back off, the conflict Zone is modified as

$$CZ_{new} = CZ_{curr} * f2(t) \qquad (2)$$

If a node receives multiple packets of the same route discovery chain, before it has transmitted any packet, it maintains independent counters for each of them. The

Packet corresponding to the first expired counter is transmitted,

The goal of the modifications is to stable delay that creates a notion of local congestion, which is a function of the trust value. A highly trusted route would incur a lower delay, thus increasing the likelihood of being used. A less trusted route would incur a higher delay, decreasing the probability of use. This is a critical difference in our approach from others. We do not impose hard thresholds on trust to drop or forward packets. In schemes where such a decision process is used, the thresholds are typically based on policy. However, this is not efficient in all scenarios and may lead to fragmentation of the network. Our policy realizes a similar threshold dynamically, to ensure full connectivity. The adjustment to the contention window increases the sensitivity to traffic congestion. The goal of the pretender is to be a part of the maximum number of routes. Even if the pretender succeeds in becoming a part of few routes, either due to lack of alternative options or the delayed evolution of trust metrics, the increase in sensitivity to traffic ensures that the number of paths it can influence does not grow much. We consider a scenario where short pretender link have been assumed nodes with non-adversarial paths to fulfill the first two objectives.

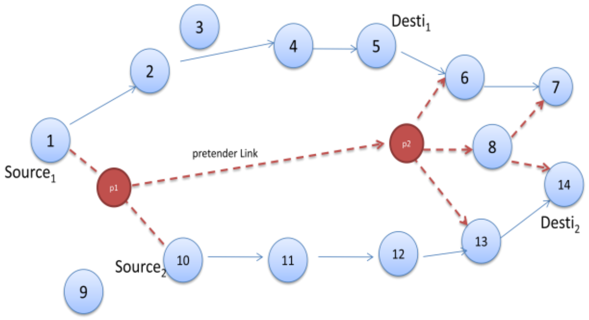

Fig2. Pretender link while pervasive nodes Communication

Well placed adversaries, p1, p2 can attract a large amount of traffic by the announcement of an alternative shorter path where Node 1 initiates a route discovery for Node 6. As a route discovery packet travels through the pretender link to Node 6 and it holds the packet for a time prior to relaying it to Node 6. The objective of the scheme is to define a delay large enough to consider the alternate path, in this case 1→2 → 4→5. It would require selecting unreasonably large delay via a malicious node, which can be inefficient due to increases the latency in all possible routes setting stages. The probability that the pretender path is selected in this, however, once this path is selected for transmitting traffic, by modifying the contention window, we ensure, that the resistance offered through Node 10, for the case of 10→14 would be larger, leading to decrease in the probability of selecting the shorter path.

For the remainder of this paper, we assume that the routing protocol used in the network is AODV. This is generally the case for most ad-hoc networks, since reactive schemes adapt better to rapid topology changes. In our scheme, we artificially increase the propagation delay of un-trusted routes to decrease the adversarial advantage. This requires the assumption that the routing schemes use congestion as a metric for route selection. The underlying property of schemes to support duplicate packet rejection, as accept only the first route request packets and discard the rest, such as in AODV. In an ideal setting such schemes aim to minimize the hop count. However, considering the underlying link layer dynamics, shorter and fastest path is selected. For trust evaluation we consider n number of packets P_n transmitted over a link, the distribution of the trust T conditioned on n is a mixed distribution as where probability P will be as per the selection of normal path or pretender path. Evaluation of the Binomial distribution with parameters (P_n, P) at point nt can be defined as

$$T= Db(P_n, P,nt) \qquad (3)$$

The parameters and the probability that packets are authenticated successfully, over a path P, different links observe different number of packets to make a trust decision. Distribution of number of packets over a link before breaking, with PN(n) representing the probability of using n packets for establishing trust, we obtain the probability density function of the trust as

$$PT=\sum_{n\varepsilon 1} \mathrm{Db}(\mathrm{Pn}, \mathrm{P}, \mathrm{nt})\mathrm{Pn}\ (n) \qquad (4)$$

Anti-Attack Trust Metrics: We put our efforts to present a quantitative framework For Anti-Attack trust metrics for a given type of attack, we assume that devices are seamlessly connected and form a graph like structure where an attacker can add or delete edges from the legitimate part of the trust graph, spotting to random nodes. These edges may point directly to nodes under the attacker's control, or perhaps to other good nodes, in order to mislead the trust metric. Here each attack is assigned a cost and typical cost metric is to count the number of edges added. Suppose an attack of a given cost, what is the highest number of bad announcement the attacker can force to be accepted? If this number is restricted, the trust metric is anti-attack. If it can grow to the same order as the number of good claims for a fairly low cost attack, then the trust metric suffers from disastrous malfunction and is not anti-attack

Attacks: Autonomous nature of the security decisions that derive from Trust computations mean that trust schemes can be the target of attacks themselves. The following are some examples of attacks that can occur:

- **Bad Mouthing Attack:** When a node might intentionally provide a bad commendation of another node.
- **Denial of Service Attack:** Trust schemes that don't rely on trust propagation, such as neighbor sensing methods do not suffer from denial of service attacks.
- **On-Off Attack:** For most of the common interactions routing a node behave correctly and when attacks occur by adding context to transactions depending on location where transaction might reduce protection over heads to against such attacks.
- **Conflicting Behavior Attack:** As with on-off attacks, when a node exhibits conflicting behavior inconsistent recommendations about other nodes over a time the performance of the trust management system would decreases.
- M**asking Attack:** An attacker will provide recommendations based on the majority verdict, and Then at times provide false information to degrade the trust scheme. Providing a greater service to honest nodes and heavily penalizing the dishonest nodes provides protection against such attacks
- **Sybil attacks:** A malicious node can create fake IDs that can take the blame for malicious actions and perform malicious attacks. In a trust scheme without a centralized control, a node is vulnerable to such attacks. Particularly trust metrics can be leveraged to reflect this, where in recommendation based systems

new nodes or nodes with little previous trust relationship history can labeled as an unknown node.

- **Agreement Attack:** In recommendation based rust scheme an agreement attack consists of more than one node cooperate with each other to provide fake information regarding about an honest node. Neighbor sensing and hybrid approaches than utilize direct trust are usually immune to such attacks. Reducing the recommendation field has been considered to reduce attacks where recommendations are confined to neighboring nodes enabling behavior changes to be identified.

Metric Cost Estimation: There are two types of cost metrics considered as first one to count the number of links added and second is to calculate the number of "attacked" nodes with added external links, and to assume that any such node may have an arbitrary number of edges added. The anti-attack conflict of different trust metrics will behave differently for any given attack, the number of nodes counted is no greater than the number of links counted. A link attack is considered to affronted entity for generating an edge. In many cases, growing such attack is simple like sending fake messages.

Edge attack: To deceive the victim once. Protection against node attack is a stronger property than protection against edge attack. Attack of a single node can correspond to an arbitrary number of edges. We analyze two classes of attacks: one in which the attacker is able to select the pretender, and another in which the pretender are chosen randomly. We find that it in most cases it is considerably more so. This result parallels the literature in scale-free networks, in which removing more effective in fragmenting the network than simply removing random nodes.

Some examples of such protocols relevant to our presentation are routing schemes such as AODV, DSR One of the critical threat to the performance of such environment is the impulsive behavior of nodes. Being highly dependent on cooperation of other nodes in the network, even a simple adversary with constrained access can cause significant scarcity. there has been tremendous research effort on developing different mechanisms to secure these networks

Performance Evaluation Mobile pervasive systems without centralized management infrastructure have been gaining popularity in the by providing widespread pervasive applications ranging from military scenarios, infrastructure monitoring and mobile healthcare by distributed processing of data. Such systems are resource restricted and broadcast nature of the communication medium and the inherent unreliability of the wireless medium. Challenges posed by these differences have led researchers, over the past two decades, to develop significantly efficient protocols customized for these systems.

The performance of the scheme and the overhead introduced are highly dependent on the choice of the functions f1( ) and f2( ). We consider candidate functions for f1( ) over a set of continuous functions such that If a node receives multiple packets of the same route discovery chain, before it has transmitted any packet.

$$D=\sum_{i=1}^{R1}(f1(ti)+d+\sum_{i=1}^{R2}f1(t_i^{\propto})+d_p \qquad (5)$$

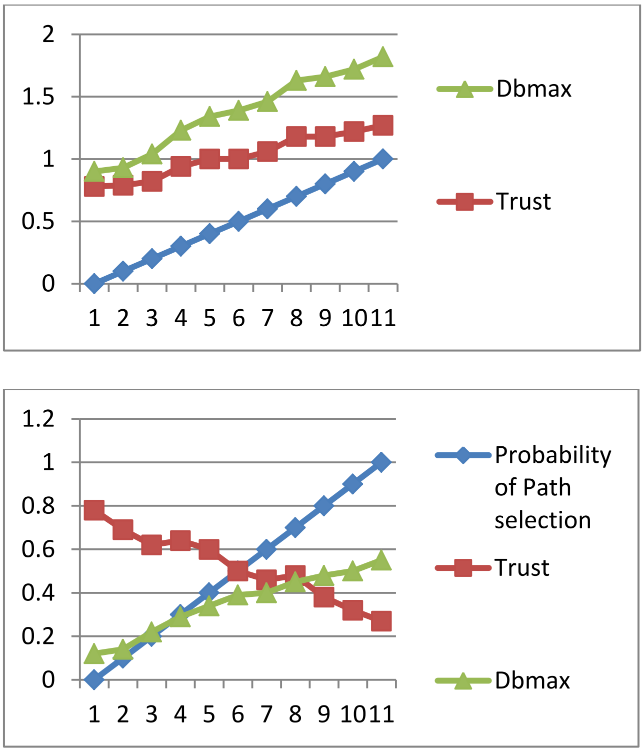

Fig.3: Distribution Delay and trust with path selection probability

Where R1 and R2 are the two alternative routes, d and d_p represents the propagation delay and processing delay. For evaluation we assume any route R, the value of N=50 packets uniformly distributed in the interval [10,500] and delay functionf1 () for trust distribution.

This can be defined as

$$f1(t)=D_{max}\frac{Db_{max}}{1+\propto e^{\beta}}$$

A highly trusted route would incur a lower delay, thus increasing the likelihood of being used. A less trusted route would. In schemes where such a decision process is used, the thresholds are typically based on policy. Our policy realizes a similar threshold dynamically, to ensure full connectivity. The advantage of our scheme is the requirement of limited network knowledge at each node. This makes our scheme particularly advantageous in networks using on demand routing.

Security analysis: The appointment mechanism of the validation of responses to queries is a good match to the guarantees provided by the group trust metric. The group trust metric can guarantee that a fraction of the total nodes accepted is good, but this is not the same as guaranteeing that a fraction of the accepted nodes responsible for a name is good.

Mobile Environment Metrics for Security: The mobile pervasive environment based on wireless, open medium for communications that can be freely available everywhere with critical security solutions as challenging task. Secured and trusted wireless is a technical challenge, having a strong effect on the global security level of MPE. Virus and worm attacks are now most common attacks but it can be predicted for future that with the growth of technology and higher dependency on MPE, the boundary-less network, the more tempting it is for the other kind of attacks. As a device at risk of being captured and hijacked, a MPE node must be protected in some way. The level of protection affects the level of security. The physical security of devices can be severely compromised in war or terrorism scenarios: nodes can be damaged or even destroyed completely.

VIII. Conclusion & Future Work

In this paper, we explore trust based soft metrics concerns requirement and challenges to decide the trust computations metric factors in mobile pervasive environment. The objective is to identify the trust parameters while routing and determine the node behavior for soft security relying on trust metric. Major contribution of our work is the utilization of resulting the trust to enhance security assurance in existing routing protocols. We rely on existing methodologies for obtain trust and certain assumptions about the routing protocol and lower layers, The proposed approaches can contribute to identify Basic Measurable Components and their relationships based on the results from threat and vulnerability analysis. We have identified the core component metric areas that have a remarkable impact on the security assurance in MPE.

References

[1] Blaze, M., Feigenbaum, J., and Lacy, J. 1996. Decentralized Trust Management. In Proceedings of IEEE Symposium on Security and Privacy, (Oakland, CA, May 1996) Online at:http://www.crypto.com/papers/policymaker.pdf.

[2] Blaze, M., Feigenbaum, J. and Keromytis, A.D. 1998. KeyNote: Trust management for public-key infrastructures (position paper). In Proceedings of 6th International Workshop on Security Protocols (Cambridge, UK, Apr. 15-17, 1998). LNCS 1550, Springer-Verlag, 1998. 59–63.

[3] Cho, J.-H., and Swami, A. 2009. Towards Trust-based Cognitive Networks: A Survey of Trust Management for Mobile Ad Hoc Networks. In Proceedings of 14th International Command and Control Research and Technology Symposium (ICCRTS) (Washington, DC, June 2009). Online at: http://www.dodccrp.org/events/papers/191.pdf.

[4] Chu, Y.H., Feigenbaum, J., LaMacchia, B., Resnick, P., and Strauss, M. 1997. REFEREE: Trust Management for Web Applications. Computer Networks and ISDN Systems 29, 8-13(Sep. 1997), 953–964. DOI=http://doi.acm.org/10.1016/S0169-7552 (97)00009-3.

[5] 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].

[6] D. McCoy, D. Sicker and D. Grunwald, "A mechanism for detecting and responding to misbehaving nodes in wireless networks," in 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON '07, pp. 678–684, 2007.

[7] Jøsang, A., Ismail, R., and Boyd, C. 2006. A Survey of Trustand Reputation Systems for Online Service Provision. Decision Support Systems 43, 2 (Mar 2007), 618-644DOIhttp://doi.acm.org/10.1016/j.dss.2005.05.019.

[8] Morton Deutsch. Trust and suspicion. Conflict Resolution, 2(4):265–279, 1958.

[9] Payne, S. C.: A Guide to Security Metrics. SANS Institute Information Security Reading Room, June (2006).

[10] Rasmusson, L., and Janssen, S. 1996. Simulated Social Control for Secure Internet Commerce. In Proceedings of New Security Paradigms Workshop (Lake Arrowhead, CA, Sep. 1996), 18- 25. DOI= ttp://doi.ac.org/10.1145/304851.304860.

[11] S. Zheng and J. Baras, "Trust-assisted anomaly detection and localization in wireless sensor networks," in Proc. IEEE Conf. on Sensor, Mesh and Ad Hoc Comm. and Netw (SECON), 2011, pp. 386–394.

[12] V. Balakrishnan, V. Varadharajan, P. Lucs, and U. K. Tupakula, "Trust enhanced secure mobile ad-hoc network routing," in21st International Conference on Advanced Information Networking and Applications Workshops, AINAW '07, pp. 27–33, 2007.

[13] X. Wang, L. Liu and J. Su, "Rlm: A general model for trust representation and aggregation," IEEE Transactions on Services Computing, vol. 99, 2010.

[14] Xavier Titi1, Carlos Ballester Lafuente1, Jean-Marc Seigneur, Trust Management for Selecting Trustworthy Access Points, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814.

[15] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 867–880, May 2012.

Author's profile

Mrs. Madhu S. Gaur is MCA, M.Tech. and Persuing P.hD. from Graphic Era University, Dehradun, Uttranchal, India and working as Associate prof. at G.L. Bajaj Intitute of Technology & Management, Greater Noida, UP India. She is serving IT industry as trainer academician and researcher from last 16+ years. Her areas of interest include Object Oriented Systems, .Net Technology and Trust Management and security in mobile computing environment.

Dr. Bhaskar Pant is Ph.D. from Maulana Azad National Institute of Technology, Bhopal, India and working as Associate Professor in the Department of Computer Science/Information Technology. His research interests in Data Mining, Machine Learning, soft Computing, Bioinformatics.