International Journal of Information Technology and Knowledge Management
January June 2009, Volume 2, No. 1, pp. 185-189

SECURITY AND REPUTATION SCHEMES IN AD-HOC NETWORKS ROUTING

Ashwani Kush*

Ad hoc networks have vital problem concerning their security aspects. These must be solved in order to realize complete Ad hoc applications. The dynamic and cooperative nature of ad hoc networks present challenges in securing these networks. There are recent research efforts in securing ad hoc networks. Amongst security approaches, there are threshold cryptography, certification authority, reputation and authentication, in this paper an introduction and survey of these approaches have been presented.

1. Security Problems

Threats can be categorized as threat sources, threat actions, threat consequences, threat consequence zones, and threat consequence periods. These attacks can be broadly classified into two main categories as: Passive attacks, Active attacks. Details have been given by many researchers as in [5,8,11,17,18,19]. Figure 1 summarizes the goals, features and architecture of a reputation system designed for ad hoc networks. In mobile ad hoc networks, nodes are both routers and terminals. For lack of routing infrastructure, they have to cooperate to communicate. Cooperation at the network layer means routing and forwarding packets. Misbehavior means [15] deviation from regular routing and forwarding. It arises for several reasons; unintentionally when a node is faulty. There is a natural incentive for nodes [15] to only consume, but not contribute to the services of the system. Intentional misbehavior can aim at an advantage for the misbehaving node or just constitute vandalism, such as enabling a malicious node to mount an attack or a selfish node to save power. The use of reputation systems in many different areas of IT is increasing, they are used to decide who to trust, and to encourage trustworthy behavior.

Resnick and Zeckhauser [14] identify goals for reputation systems:

(1) To provide information to distinguish between a trustworthy principal and an untrustworthy principal.

(2) To encourage principals to act in a trustworthy manner.

The features of a reputation system can be classified as follows:

Representation of information and classification: These determine how monitored events are stored and translated into reputation ratings, and how ratings are classified for response.

Use of second-hand information: Reputation systems can either rely exclusively on their own observations or also consider information obtained by others. Second hand information can, however, be spurious, which raises the questions of how to incorporate it in a safe way and whether to propagate it.

Trust: The use of trust influences the decision of using second-hand information. The design choices are about how to build trust, out-of-band trust versus building trust on experience, how to represent trust, and how to manage the influence of trust on responses.

Redemption and secondary response: When a node has been isolated, it can no longer be observed. The question of how those nodes should be rated over time is addressed by these two features. If the misbehavior of a node is temporary, a redemption mechanism ensures that it can come back to the network. It is, however, desirable to prevent recidivists from exploiting a redemption mechanism. This can be achieved by secondary response, meaning a quicker response to a recurring threat, in analogy to the human immune system. To enable nodes to adapt to changes in the network environment caused by misbehaving nodes, a detection & reputation system consists of three modules, Detection, reputation and response modules. The goal of detection is to gather first hand information about the behavior of nodes in a network. The two main ideas behind reputation are; that it is used as an incentive for good behavior and provides a basis for the choice of transaction partners. The response aims at isolating misbehaving nodes.

This isolation has three purposes. The first is to reduce the effect of misbehavior by depriving the misbehaving node of the opportunity to participate in the network. The second is to serve as an incentive to behave well to not be denied service. Finally, the third is to obtain better service.

* Department of Computer Science, University College, Kurukshetra University India, *E-mail: akush20@gmail.com*

This work is part of the project Sponsored by UGC INDIA Project on Security in Wireless Ad hoc Networks

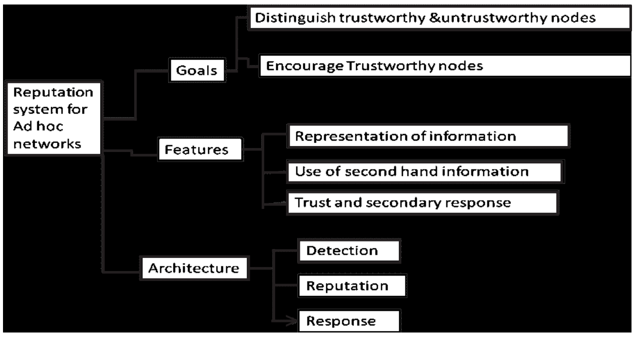
Reputation system for Ad hoc networks
Goals
Distinguish trustworthy &untrustworthy nodes
Encourage Trustworthy nodes
Features
Representation of information
Use of second hand information
Trust and secondary response
Architecture
Detection
Reputation
Response

Figure 1: Goals, Features and Architecture of an Ad Hoc Networks Reputation System

2. Security Solutions

This section focuses on the reputation and trust schemes that have been suggested for ad hoc networks and give a survey of these schemes. In A Dynamic Trust Model for Mobile Ad Hoc Networks [22]; a trust model for mobile ad hoc networks was introduced. Initially each node is assigned a trust level. Several approaches are used to dynamically update trust levels by using reports from threat detection tools, such as Intrusion Detection Systems (IDSs), located on all nodes in the network. The nodes neighboring to a node exhibiting suspicious behavior initiate trust reports. These trust reports are propagated through the network. A source node can use the trust levels it establishes for other nodes to evaluate the security of routes to destination nodes. Using these trust levels as a guide, the source node can then select a route that meets the security requirements of the message to be transmitted. In Local Detection of Selfish Routing Behavior in Ad Hoc Networks [3], a method to distinguish selfish peers from cooperative ones has been developed based solely on local observations of AODV routing protocol behavior. The approach uses the finite state machine model of locally observed AODV actions to build up a statistical description of the behavior of each neighbor. A series of well known statistical tests to features derived from this description are applied to partition the set neighboring nodes into a cooperative and selfish class. A node can have a reputation value about a subject without ever having interacted with it himself. However, an inherent problem with any such mechanism is the vulnerability to liars. Untrustworthy nodes can have different strategies to publish their falsified first-hand information when attempting to influence reputation ratings (e.g., when they want to discredit regular nodes). In Self-Policing Mobile Ad Hoc networks by Reputation Systems[15] Liars may also use the following strategies:

Brain washing: When a node is surrounded by combining lying nodes, it can be tricked into believing false information. When it later moves into a different neighborhood with honest nodes, it will not believe them since their information deviates too much from its own.

Intoxication: Nodes could try to gain trust from others by telling the truth over a sustained period of time and only then start lying.

Identity spoofing: Without identity persistence, a badly rated node could disappear and reappear with a different identity. By using second hand information, an accurate estimate of some subject's behavior can be obtained faster.

A first step to the analysis of a reputation system based on a deviation test was presented in Analysis of a Reputation System for Mobile Ad-Hoc Networks with Liars [8]. Nodes accept second hand information only if this does not differ too much from their reputation values. Direct observations are always accepted and the reputation values updated accordingly. An indirect (second hand) observation arises from interactions with peers who report about their own direct observations. Indirect observations are only accepted if the reported observation does not deviate too far from the current reputation. To keep a history of previous events, two counters, are updated whenever there is a new observation, either direct or indirect. One of them tracks positive observations, and the other keeps track of negative observations. Direct observations are always accepted and counted with indirect observations have to pass a deviation test [8]. In Towards Node-Level Security Management in Self-Organizing Mobile Ad Hoc Networks [13], elements of a monitoring scheme in MANETs have been presented. It has been stated that a security monitoring system continuously estimating the actual security level can be attached to individual nodes. There are two separate goals in estimation process in [13]: security level of node and security level of network.

Another collaborative mechanism for detecting malicious incorrect packet forwarding attacks was described in A Reputation-Based Trust Mechanism for Ad Hoc Networks, [20]. The proposed model provides two main functionalities: monitoring the behaviour of the neighboring nodes in the network and computing their reputations based on the information provided by the monitoring. In this a trust manager protocol collaboration between neighboring nodes is required. Mechanism builds trust through the trust manager. As it is shown in Figure 2, there are two main modules; the monitoring module and the reputation handling module. In the monitoring module, each node independently monitors its neighboring nodes forwarding activity. Monitoring is related to the proportion of correctly forwarded packets during a fixed time window. If anomaly is detected, monitor informs the reputation manager. The reputation handling module consists of four components, the first is the reputation collecting through sensing or direct monitoring or recommendations& accusations using on demand technique or proactive broadcasting technique. The second component is the reputation formatting which uses a reputation template containing different fields. The reputation information has to be evaluated before it is locally stored or broadcasted to the neighborhood. That is why in the reputation maintenance, each node is assumed to maintain a reputation table for storing its one hop neighborhood reputation information that it gets by direct monitoring or through broadcast from some neighboring nodes. In the last, reputation rating module, the most recent reputation is always considered heavier.

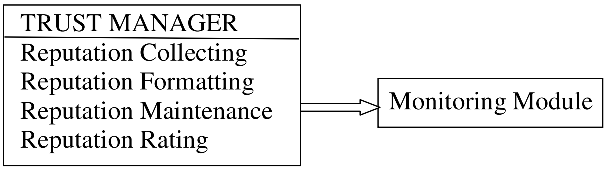

Figure 2: Trust Manager Architecture

The performance of three trust-based reactive routing protocols in a network with varying number of malicious nodes was evaluated in Performance Comparison of Trust-Based Reactive Routing Protocols [1]. Every time a node transmits a data or control packet, it immediately brings its receiver into the promiscuous mode so as to overhear its immediate neighbor forwarding the packet. Two categories could be derived to compute direct trust: the first category is acknowledgment, provides with information concerning black hole, modification, attacks and the second category is packet precision for data integrity. The trusted update interval has been proved to be a very critical component, it determines the time a node should wait before assigning a trust level. In [1], each trust category is represented by one or more types of events. The successful and failed events of all categories are represented in tables, and all events are then normalized to produce usable information having statistical properties. The normalized value of one of the events used in the computation of a category is calculated a function of a failed and successful events. Trust values from the two trust categories are the assigned weights according to their priorities in order to determine the direct trust level of a particular node. A scheme for evaluating trust evidence in ad hoc networks was presented in On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks, [5]. It is entirely based on information originating at the users of the network. No centralized infrastructure is required, although the presence of one can certainly be utilized. Also, users need not have personal, direct experience with every other user in the network in order to compute an opinion about them. They can base their opinion on second hand evidence provided by intermediate nodes, thus benefiting from other nodes' experiences. At each round of computation, the source node computes opinions for all nodes. This means that information acquired at a single round can be stored and subsequently used for many trust decisions. If there is not enough evidence to determine an opinion, then no opinion is formed. So, when malicious nodes are present in the network they cannot fool the system into accepting a malicious node as benevolent. The trust inference problem was viewed as a generalized shortest path problem on a weighted directed graph $G(V, E)$. Each opinion consists of two values: The trust value, and the confidence value and both the trust and confidence value are assigned by the issuer, in accordance to his own criteria (very strict, less strict, etc…). The opinions are updated as the topology changes. Two versions of trust influence problem: Finding the trust confidence value & the highest trust value among all trust paths. Two operators are used to combine opinions: one operation combines info among a path; the other combines across paths, then these operators can be used for a general framework for solving path problems in graphs. Finally, semirings are used as models for trust computation. Figure 3 depicts the overall scheme that was presented in [5].

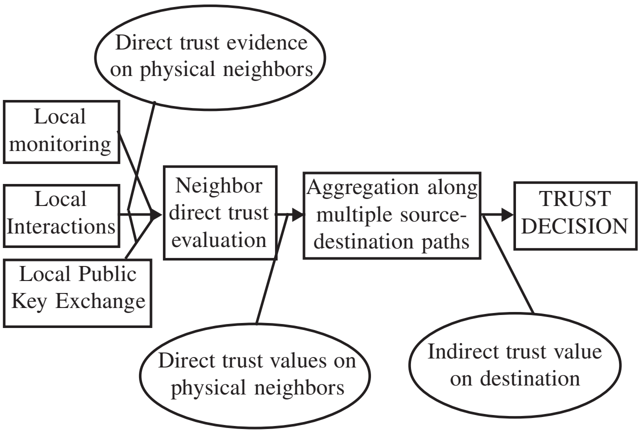
Direct trust evidence on physical neighbors
Local monitoring
Local Interactions
Local Public Key Exchange
Neighbor direct trust evaluation
Aggregation along multiple source-destination paths
TRUST DECISION
Direct trust values on physical neighbors
Indirect trust value on destination

Figure 3: Trust Evidence Scheme [5]

In Security and Cooperation in Clustered Mobile Ad Hoc Networks With Centralized Supervision [16], a node reputation scheme aiming at reinforcing node cooperation in MANETs with centralized control has been presented. This scheme has been designed for centralized ad hoc network architecture, an ad hoc enhancement to the HIPERLAN/2WLANstandard. Misbehavior detection techniques for protocol attacks in both the cluster formation and data transmission phases of the network operation has been developed. Statistical methods for selecting the optimal parameters of the reputation scheme were investigated and their efficiency has been illustrated through theoretical analysis and simulation results. In Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks [6], a secure random reporting protocol for a civilian ad hoc network has been proposed. In this protocol, the source and destination collect reports from intermediate nodes on the routing path. Every data packet initiates a report from one intermediate node that is randomly chosen by a source node. Through a symmetric cryptographic construction, the node selection is not disclosed to other intermediate nodes. The random reporting protocol has three modes: the basic periodic reporting, the random reporting node selection, the random reporting node and direction selection, and the random bidirectional selection. Although the report is securely transmitted to the destination, it is not guaranteed to be accurate, since nodes may cheat in order to get credit. A chained scheme has been devised on the link layer acknowledgments to verify the validity of the received report. From both security and performance perspectives, the secure random reporting protocol is advantageous for gathering the forwarding activities of mobile nodes in civilian ad hoc networks. The report can be used for determining whether congestion exists in network, engineering the traffic, crediting nodes with how many packet they relayed, and detecting that nodes maliciously drop packets.

3. Proposed Solutions

The hardware constraints of ad hoc networks are in terms of:

(1) **Cost**: nodes are generally not tamper-resistant.

(2) **Space**: They can only store as many keys as are usually allowed by the storage left over by the operating system and application code, which is not much.

(3) **Energy**: It is necessary to optimize the use of cryptography since cryptographic operations tend to be resource-intensive.

(4) **Time**: Public-key cryptography should be avoided or at least limited to applications which are not time-constrained, because they are a few order of magnitude more resource *and* time consuming than symmetric-key cryptography.

The security and functional requirements of most ad hoc networks are such that under the above constraints, the following guidelines need to be taken into account:

(1) *No Single Key*: The system should not operate on a system-wide key (or keys). Due to the sensor nodes' lack of tamper-resistance, having a vulnerable system-wide key is *not* better than having no key at all.

(2) *No Single Point*: The system should not have a single point (e.g. node) of failure.

(3) *Scalability:* The system should be scalable in the sense that the addition of new nodes should not cause excessive rise in computation, communication and administrative overhead in the network.

As of writing, we are not aware of any key management architecture that satisfies all the above hardware constraints as well as the guidelines. Some of the popular solutions have been discussed here as:

(a) Virtual Private Networks (VPN)[7, 16]: This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP (Internet Protocol) data grams. Software are available to implement VPNs on just about every platform. Authentication depends upon three factors as password, Fingerprints and a security Token. Using two factors is desirable and using all three is most secured. VPN only support IP suite so it cannot be solution for all environments.

(b) Encryption[4,10]: Encryption is a technique used for many years for passing information from one place to other in a secured manner. A message in its original shape is referred to as a plaintext (or Text) and a message used to conceal original message is called Ciphertext (or Cipher). The process of changing plaintext into ciphertext is called Encryption and the reverse process is called decryption. There are many algorithms available for these processes. Some of them are Data Encryption Standard (DES), International Data Encryption algorithm (IDEA) and Public key algorithm (RSA) These are based on key based algorithms. There is one popular key algorithm as Digital signature algorithm. In Digital signature, Signer encrypts the message with key, this is sent to recipient, the message is then decrypted with sender's public key. In case of ad hoc networks this may not be the best method as it uses a lot of space and is also slow.

(c) One Way Hash Function[7]: There is another algorithm called One way hash Function: it is like checksum of a block of text and is secure in that it is impossible to generate the same hash function value without knowing the correct algorithm and key. It accepts a variable size message and produces a affixed size tag as output. This algorithm can be combined with encryption to provide an efficient and effective digital signature.

(d) Digital Signature[14]: External attacks can be checked using Confidentiality of the routing information and also by authentication and integrity assurance features. Encryption can be solution to this. Digital signatures and one way functions can be applied. Permian used complex robustness to protect routing data from compromised nodes. It is ability to continue correct operation in presence of arbitrary nodes with complex failures.

4. CONCLUSIONS AND CHALLENGES

In this paper some of the security approaches used for securing ad hoc networks has been surveyed. These are approaches the threshold cryptography, certification authorities, reputation and trust, and authentication. There are still many challenges and research openings in the area of ad hoc networks security.

Moreover, a lightweight method for propagating the revocation news needs to be investigated to decide whether the periodic announcement or the on demand is more suitable in the case of ad hoc networks. The different reputation and trust based schemes that have been proposed for ad hoc networks in the literature has been surveyed ranging between collaborative and independent node based schemes. Several reputation schemes can be modified or blended together to enhance their performance and obtain an optimum scheme that is suitable to the ad hoc networks very specific characteristics. Some of the authentication schemes proposed in the literature need to be combined with other security schemes like reputation and trust based schemes.

References

[1] A. Pirzada, C. McDonald, and A. Datta, "Performance Comparison of Trust-Based Reactive Routing Protocols," *IEEE Transactions on Mobile Computing*, **05**, (6), (June, 2006), 695–710.

[2] A. Kush, P. Gupta, A. Pandey, C. J. Hawang, "Power Aware Virtual Node Routing Scheme in Ad Hoc Networks", *IASTED International Conference on Wireless Networks and Emerging Technologies (WNET 2004)*, Banff, Canada, 698–704, (July 2004).

[3] B. Wang, S. Soltani, J. Shapiro, and P. Tan. "Local Detection of Selfish Routing Behavior in Ad Hoc Networks," *ISPAN*, *8th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'05)*, (2005), 392–399.

[4] C. Parkins and E. Royer, "Ad Hoc on Demand Distance Vector Routing", *2nd IEEE Workshop on Mobile Computing*, (1999), 90–100.

[5] G. Theodorakopoulos and J. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, **24**, (2), (February 2006).

[6] H. Choi, W. Enck, J. Shin, P. McDaniel, and T. La Porta, "Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks," *Mobiquitous*, *The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, (2005), 12–21.

[7] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad hoc Wireless Networks," In *Proceedings of 7th IEEE Symposium on Computers and Communications (ISCC '02)*, (July 2002).

[8] J. Mundinger, J. Le Boudec. "Analysis of a Reputation System for Mobile Ad-Hoc Networks with Liars," *Wiopt*, *Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05)*, (2005), 41–46.

[9] L. Zhou and Z. J. Haas, "Securing Ad hoc Networks", *IEEE Network Magazine*, **13** (6): 24–30, (November/December 1999).

[10] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", IETF MANET List, Available at draft-guerrero-manet-saodv-03.txt., March 18, 2005.

[11] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile ad hoc Networks", *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002),* (Jan 2002).

[12] R. Hauser, A. Przygienda, and G. Tsudik, "Reducing the Cost of Security in Link State Routing", *In Symposium on Network and Distributed Systems Security* (NDSS '97), San Diego, California, . Internet Society, (Feb. 1997), 93–99.

[13] R. Savola, and I. Uusitalo, "Towards Node Level Security Management in Self-Organizing Mobile Ad Hoc Networks," AICT-ICIW, *Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW'06)*, (2006), 36.

[14] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Communications of ACM*, **21** (2), (Feb. 1978), 120–126.

[15] S. Buchegger, and J. Le Boudec, "Self-Policing Mobile Ad Hoc Networks by Reputation Systems," *IEEE Communications Magazine*, **43**, (7), (July 2005).

[16] S. Vassilaras, D. Vogiatzis and G. Yovanof, "Security and Cooperation in Clustered Mobile Ad Hoc Networks With Centralized Supervision," *IEEE Journal on Selected Areas in Communications*, **24**, (2), (February 2006).

[17] T. Karygiannis and L. Owens, "Wireless Network Security", *NIST Special Publication* 800-48**,** (November 2002).

[18] William Stallings, "Cryptography and Network Security: Principles and Practice". Second Edition, 3–12.

[19] Y. C. Hu, A. Perrig and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks", *Technical Report* TR01-383, Rice University, (Dec. 2001).

[20] Y. Rebahi, V. Mujica, and D. Sisalem. "A Reputation-Based Trust Mechanism for Ad Hoc Networks," ISCC, 37–42, *10th IEEE Symposium on Computers and Communications* (ISCC'05), (2005).

[21] Yonguang Zhang and Wenke Lee, "Intrusion detection in Wireless ad-hoc Networks", *In 6th International Conference on Mobile Computing and Networking(MOBICOM'00)*, (Aug 2000), 275– 283.

[22] Z. Liu, A. Joy, R. Thompson. "A Dynamic Trust Model for Mobile Ad Hoc Networks," FTDCS, 80–85, 1*0th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04)*, (2004).