

An Energy Aware Secure Data Transmission In Manet's Using Direct and Indirect Observation

Subash Chandar¹, Thalir Mathi², Lavanyah³

¹Assistant Professor, ^{2,3}Students

^{1, 2,3}Department of Computer Science and Engineering

Jeppiaar Engineering College, Chennai

subashchandar@gmail.com, thalir03@gmail.com, surthi.lavanyah777@gmail.com

Abstract

Mobile devices that can dynamically move and reorganize themselves and communicate over wireless links form MANET. Because of the importance of routing protocols in dynamic multi-hop networks, a lot of mobile ad hoc network routing protocols have been proposed. The basic features of mobile ad hoc networks (MANET's) are dynamic topology and open wireless medium. These features will lead to security attacks. A trust management scheme based on direct and indirect observation is developed to enhance the security in MANET's. But the problem is trust management scheme does not provide secure transmission in MANET's. A new security mechanism is proposed to ensure security in MANET's. The proposed work is implemented with AODV protocol. This AODV protocol is implemented with the trust management scheme for direct and indirect observation of nodes. These observations are used to identify and prevent the compromised or malicious nodes in the network and also to prevent from security issues such as malicious node attacks, misbehavior of nodes such as dropping or modifying packets during transmission. Further the proposed scheme will be useful for secure data transfer, security, increase network performance, and avoid congestion and hidden terminal situations.

Keywords: MANET, Security, AODV, Trust Management.

Introduction

With recent advances in wireless technologies and mobile devices, Mobile Ad hoc Networks (MANETs) have become popular as a key communication technology in military tactical environments such as establishment of communication networks used to coordinate military deployment among the soldiers. A mobile network or cellular network is a radio network consists of spatially divided cells across some regions.

Each cell is fixed with a base station and user in the region will communicate by this base station. There are three types of wireless mobile networks they are, Global system for mobile communication (GSM), Personalized Communication Service (PCS) and Digital Advanced Mobile Phone Service. MANET's are a kind of Wireless ad hoc network that usually has a routable Networking environment on top of a Link Layer ad hoc network. MANET's consist of a self-forming, self-healing and peer to peer network in contrast to a mesh network has a central controller (to estimate, optimize, and distribute the routing table). There are many risks in military environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless transmission And distributed nature, absence of centralized infrastructure for security protection. Therefore, security in tactical MANETs is challenging research topic. There are two complementary classes of approach that can safeguard tactical MANETs: prevention-based and detection-based approaches.

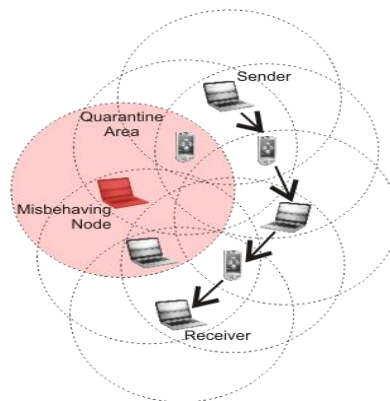


Figure 1.1: Path Determination

One issue of these prevention-based approaches is that a centralized key management which requires infrastructure, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields. If the infrastructure is destroyed security in tactical MANETs is a challenging research topic. There are two complementary classes of Mobile Ad hoc Networks (MANETs) have become popular as a key communication technology in military tactical environments such as establishment of communication networks used to coordinate military deployment among the operational command centers. Furthermore, although prevention-based approaches can prevent misbehavior, there is a possibility for malicious nodes to participate in the routing procedure and disturb proper routing establishment. From the experience in the design of security in wired networks, many levels of security mechanisms are needed. In Mobile Adhoc Networks, this is true given the low physical security of mobile networks. It serves as the second wall of protection; detection-based algorithm can effectively help to identify malicious activities. Although some excellent work has been done on detection based approaches based on trust management in MANETs, most of the

existing approaches do not exploit direct and indirect observation (also called secondhand information that is obtained from third party nodes) at the same time to evaluate the trust of an observed node. Moreover, indirect observation in most approaches is only used to assess the reliability of nodes, which are not in the range of the observer node. Therefore, inaccurate trust values may be derived. In addition, most methods of trust evaluation from direct observation do not differentiate data packets and control packets. However, in Mobile Adhoc Networks, control packets are usually more important than data packets.

Related Work

A unified trust management scheme is implemented in MANET's to provide security using uncertain reasoning. The existing trust scheme has two components they are trust from direct observation and trust from indirect observation. In direct observation, the trust value of observed node is derived using Bayesian inference, which is a classification of uncertain reasoning when the full probability model can be defined. In indirect observation, the trust value of neighbor nodes of the observer node is derived using the Dempster-Shafer theory, which is another classification of uncertain reasoning when the proposition of interest can be derived by an indirect method. The existing scheme differentiates data packets and control packets, and meanwhile excludes the other causes that result in dropping packets, such as unreliable wireless connections and buffer overflows. It uses OLSR protocol to evaluate the trust management scheme in the Node. A distributed hierarchical key management scheme is proposed in which nodes can get their keys updated either from their parent nodes or a threshold of child nodes. The selection process of dynamic nodes is formulated as a stochastic problem and this scheme can select the best nodes to be used as private key generator PKG's from all available ones considering their security conditions and energy states. Simulation results shows that this scheme can decrease network compromising probability and increase network lifetime in tactical MANET's [3]. Main drawback of this paper is, the node selection is formulated as a stochastic restless bandit problem. This problem is solved by primal dual heuristic and divides the key update process into offline and on-line components, which reduce the computation complexity significantly. The off-line priority index computation may not work well in dynamic environment. More work should be concentrated to minimize off-line priority index computation. [1] A game-theoretic approach is proposed to quantitatively analyze the attack strategies of the attacker to make a rational decision on relay selection and the authentication parameter adaptation to reach a trade-off between security and QoS in CO-MANET's. Simulation results show the effectiveness of the proposed approach for security and QoS co-design in CO-MANET's. The main drawback of this technique is the game theoretical approach with cooperative communications enables the system to strategically select its relay by dynamically updating its belief in the maliciousness of relays according to its record of attacks. Simulation results show the effectiveness of the proposed dynamic game-theoretic approach. [2] A dynamic approach for addressing security issues and articulates why and how the ID-based cryptography can be effectively applied to

address various security problems in the resource-constrained wireless networks. An ID-based Public Key Cryptography (ID-PKC) is proposed in resource-constrained wireless ad hoc networks and hopes to solve the computational complexity of the pairing operations in the network. [4]Secure Protocol for Reliable Data Delivery (SPREAD) protocol will transform a secret message into many shares, and then deliver the shares via many paths to the destination so that even if a certain number of message shares are compromised, the secret message as a whole is not compromised. Simulation results show that the SPREAD can provide more secure data delivery when messages are transmitted across the insecure network. This mechanism enhances the security service but it alone cannot completely guarantee data confidentiality without incorporating any underlying encryption scheme and/or LPI/LPD (low probability of interception/low probability of detection) schemes at the physical layer. In particular, it is more resilient to compromised nodes problem. A redundant SPREAD scheme can be designed in such a way that a certain degree of reliability can be provided without sacrificing the security.[5]An Anonymous Overlay System for MANET's is proposed which provides provably strong source and destination anonymity under a rather strong adversary model. AOS differs from other systems for MANET's in three aspects by, it is an overlay system independent of the underlying MANET protocol stack, it resolves the conflict between anonymous communications and secure routing in MANET's and enables providing both at the same time. AOS is independent of MANET protocol stack, can coexist with indispensable secure MANET routing schemes, and can provide differentiated anonymity protection to MANET nodes with diverse anonymity requirements. The efficiency of AOS in offering strong source and destination anonymity has been theoretically proved and evaluated with numerical results. But AOS is not evaluated using network simulations and experiments.

Frame Work of The Proposed Scheme

The proposed system also uses trust management scheme from direct observation and indirect observation of nodes. Direct observation of node is derived using Bayesian inference, which is a classification of uncertain reasoning when the full probability model can be defined. Indirect observation of nodes is done by using Dempster-Shafer theory, the proposed system uses the AODV protocol, which is used to find the shortest path by sending request response messages. AODV is implemented with link metrics and trust management scheme to observe the nodes directly or indirectly. In this work we extend the energy awareness of the nodes which are participating in the network. In normal AODV it will always choose shortest path. So the nodes will lose its energy in quick manner. From our new scheme we will extend trust aware with energy aware AODV protocol. While data forwarding, the nodes will change the path based on energy level of every nodes. So we can improve the QOS with improved Security. Finally we can improve prolong network. In this Paper we use uncertain reasoning theory which is the part of artificial intelligence. In uncertain reasoning we use two methods; they are Bayesian inference and Dempster Shafer theory. The frame work of the proposed scheme consists of the Trust Scheme, Networking and

Application layer. With these three layers we are able to send the packets securely to the destination node. The data packets and the control packets are transmitted by using AODV protocol. Data packets are packets which comprises of only the data and header. Control packets are a packet which comprises of the header and flags. In this method the reliability for data packets is concentrated the more rather than the control packets.

Algorithm

To send data packets and control packets in a secured path we should find out the trust values, for determining the trust values first we have to deploy the nodes and set source and destination. Below algorithm is used to find out the secure path to send the packets.

Step1: Deploy MANET nodes in the network

Step2: Implement AODV protocol and find shortest path

Step3: Transmit sample data to destination node

Step4: Calculate Trust Value.

$$T = \lambda T^D + (1 - \lambda) T^I$$

[D=Direct observation values

I=Indirect Observation Values

λ =Weight of Trust values Based on Direct Observation]

Step5: Directly observe the neighboring nodes using Bayesian algorithm

$$f(\theta, y | x) = [p(\theta, y) f(\theta, y)] \div [p(x | \theta, y)]$$

Step6: Calculate the belief function of other nodes.

$$bel(B) = \sum_{A \subseteq B}^{\infty} m(A)$$

(Where A and B are Nodes)

Step7: Indirectly observe the node using other nodes information using Dempster-Shafer theory.

$$bel(b) = bel_1(B) \oplus bel_2(B)$$

Step8: Before transmission calculate the energy level of nodes in the paths.

$$Energy = tx \text{ Power} \times (\text{packet size}/\text{bandwidth})$$

Step9: Transmit the data in the energy efficient path.

Trust Model

The trust values can be estimated by using the direct and indirect observation. Then after finding the trust values then these values are updated in the trust repository. The trust repository comprises of all the trust values estimated for each node. After the evaluation and updating the trust values in the trust repository, then the routing takes place Initially Deploy a no of MANET Nodes. Assume distance and energy level to all these nodes. Select the source and destination node. Once the energy level and distance is assumed select the source and destination node for data transmission. After

the selection of source and destination AODV protocol is implemented to find the paths between source and destination. This protocol sends the request message to the destination node. The destination node sends the response message to the source node.

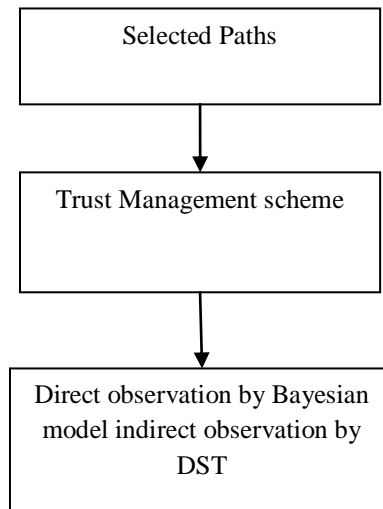


Figure 2: Trust Management Scheme

From these RR message the paths from the source to destination is selected. On the selected paths the trust management scheme is implemented to find the attacker or the compromised node in the selected path. Determine a trust value and observe the path in direct and in indirect manner. The direct observation is calculated using Bayesian model and indirect observation is calculated using Dempster Shafter theory. From the trusted value the direct and in-direct observation on path is done to find the compromised or attacker node in the path. The attacker node in the path if found from this observations. Now calculate the energy in the selected paths. Transmit the data in the higher energy path.

Platform

One of the most convincing reasons to move to java is its platform independence. Java runs on most major software and hardware platforms, including windows 98, 95, and NT Macintosh and several varieties of UNIX. Java is a general USA in 1991. Originally called oak by James Gosling, one of the inventors of the language. The java development team which included Patrick Naught on discovered that the existing language like C and C++ had limitations in terms of both reliability and portability. However, they shaped their new language java on C and C++ but removed a number of features of C and C++ that were considered as sources of problems and thus made java a really reliable, simple, portable and powerful language. Specifically, this overview will include a bit include a bit of the history of java platform, touch of the java programming language, and the ways in which people are using java applications and applets, now and in the likely future. After going a while down the

path of consumer – electronics devices, they realized that they had something particularly cool in the java language and focused on it as a language for network computing. Sun formed the java soft group which in a little over three years has grown to over six hundred people working on java related technologies. Java Swing is a Library/toolkit released by SUN Microsystems as a part of Java Language which enables Java Programmers to create GUI and rich client applications. Swing is the primary Java GUI widget toolkit. It is a part of Oracle's Java Foundation Classes (JFC) – an API for providing a graphical user interface (GUI) for Java programs. Swing was developed to provide a more suave set of GUI components than the earlier Abstract Window Toolkit. Swing provides native look and feels that emulates the look and feel of several platforms and also supports a pluggable look and feel that allows applications to have a look and feel unrelated to the underlying platform. It has more vibrant and flexible components than AWT. In addition to familiar components like buttons, check box and labels. Swing provides several advanced components like trees, tables, tabbed panel, scroll panes and lists. Unlike AWT components, Swing components are not implemented by the platform-specific code. Alternatively they are written entirely in Java and therefore are platform-independent. The term “lightweight” is used to describe such an element.

Results and Discussions

The output of the proposed scheme is generated by using the AODV protocol. The efficacy of the proposed scheme is estimated in an insecure environment. First we have to deploy the nodes for the Adhoc networks. Then we have to select the source and destination. We can deploy as many numbers of nodes. The nodes are created by giving the distance and range for the creation of nodes. Thus the MANET deployment of nodes and selecting the source and destination nodes is done. After this the implementation of AODV protocol is done. Request message is sent from the source to destination. From that the shortest route is selected and the response message is sent. After the path is selected then have to implement the Trust Management scheme. In the Trust management scheme it comprises of both direct and indirect observation. Direct observation is calculated by Bayesian inference model and indirect observation is calculated from DST. After finding the direct observation and indirect observation values, the energy aware path should be selected and then the data should be transmitted via this path. To find the energy efficient path first CBR (Constant Bit Rate) traffic is generated in all the nodes.

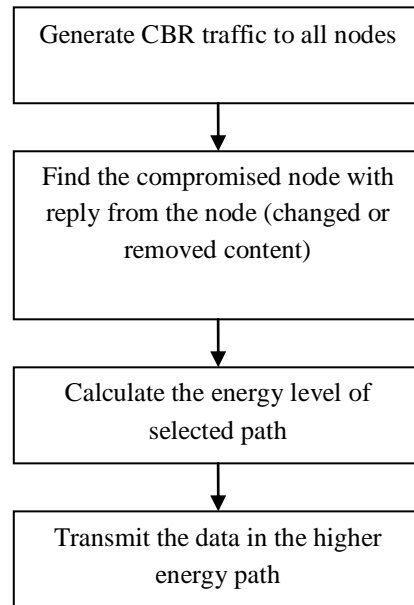


Figure 3: Transmission of Data

Then the compromised node is found out. Afterwards calculate the energy of the selected path. After the selection of the path then the data are transmitted via the path which has highest energy. Fig.2 represents the trust management scheme is implemented in the shortest selected paths and then the Bayesian inference model and Dempster Shafer theory is implemented in the trust management scheme. In the proposed scheme end to end delay is minimized and higher level of security is guaranteed. In the existing system the throughput of the nodes is low, but in the proposed system the throughput is really high. This is mainly due to the AODV protocol, AODV is a reactive protocol.

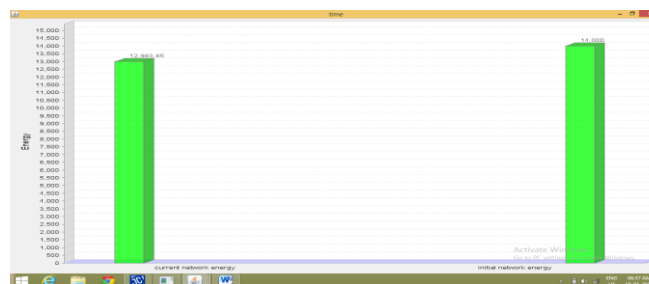


Figure 4: Energy of total Network

AODV protocol plays a key role and therefore the packet is delivered with high throughput and the end to end delay is minimized. In the Fig 3 the graph represents the throughput of the existing and the proposed system. In the existing system the throughput is quite low, but in the proposed system the throughput is maximum. Packet delivery ratio is high in proposed system compared to that of existing system.

Number of malicious nodes is detected easily in proposed system compared to that of existing system.

Conclusion

This method presents an efficient secure data transmission of data in MANET'S. First the path from the source and destination node is selected using AODV protocol. Source node sends sample data to destination node in the selected path between source and destination. After transmission the source node is the observer node it observes neighbor nodes in the path directly using Bayesian algorithm and indirectly by metrics with other neighboring nodes using Dempster Shafer theory. From the observations the compromised node or attacker node is found out and the source node transmits the data in the energy efficient path. The obtained result shows that this method provides an efficient trust management scheme and efficient transfer secure data in MANET's in energy aware path. The data is transmitted only in the path which has highest energy. Thus the data is transmitted in a secured path with highest energized route.

References

- [1] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," *EURASIP J. Wireless Communication. Networking*, vol. 2013, pp. 188–190, July 2013.
- [2] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Comm.*, vol. 16, no. 2, pp. 24–30, 2009.
- [3] F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Trans. on Network and Service Management*, vol. 7, pp. 258–267, Dec. 2010.
- [4] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: improving network security by multipath routing in mobile ad hoc networks," *ACM Wireless Networks*, vol. 15, no. 3, pp. 279–294, Mar. 2009.
- [5] R. Zhang, Y. Zhang, and Y. Fang, "AOS: An anonymous overlay system for mobile ad hoc networks," *ACM Wireless Networks*, vol. 17, no. 4, pp. 843–859, May 2011.
- [6] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On data centric trust establishment in ephemeral ad hoc networks" *Proceedings of IEEE INFOCOM'08*, (Phoenix, AZ, USA), Mar. 2008
- [7] R. Changiz, H. Halabian, F. R. Yu, I. Lambadaris, H. Tang, and P. Mason, "Trust establishment in cooperative wireless networks," in *Proc. IEEE Milcom'10*, (San Jose, CA, USA), Nov. 2010.
- [8] T. Clausen, C. Dean, and J. Dean, "Mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP)," *IETF RFC 6130*, Apr. 2011.

- [9] T. Clausen and U. Herberg, "Vulnerability Analysis of the optimized link state routing protocol version 2 (OLSRv2)" Proceedings of IEEE WCNIS 10, Feb. 2010
- [10] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey on trust and reputation management systems in wireless communications," Proceedings of the IEEE, vol. 98, no. 10, pp. 1755–1772, 2010