ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Trusted-Group Criteria for Performing Trust Aware Routing in Mobile Networks

Beenu Shokeen
[1]Computer Science and Engineering Department
PDM College of Engineering
Bahadurgarh, Haryana
bnshokeen2@gmail.com

Rashmi Kushwah
[2]Assisstant Professor of Information Technology
PDM College of Engineering
Bahadurgarh , 124507, Haryana
rashmi.31130@gmail.com

Abstract: Security in Wireless Network is the most important concern for the basic functionality of network. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. A Mobile network is one of the most widely open network in which any intruder or the selfish node can easily perform an attack and affect the communication reliability. The presented work is about to define an effective and trustful communication approach over the network. . In this approach, a group management approach is defined. Each group will be managed by the base station itself. The group authentication will be done based on Diffie-Hellman algorithm.

Key-words: Group Adaptability, Group Key Authentication, Route Generation.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. It is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently; each must forward traffic unrelated to its own use, and therefore be a router. The MANET network enables servers and clients to communicate in a non-fixed topology area and it's used in a variety of applications and fast growing networks.

With the increasing number of mobile devices, providing the computing power and connectivity to run applications like multiplayer games or collaborative work tools, MANETs are getting more and more important as they meet the requirements of today's users to connect and interact spontaneously.

Adhoc networks do not rely on any pre-established infrastructure and can therefore be deployed in places wih no infrastructure. this is useful in disaster recovery situations and places with non-existing or damaged communication infrastructure where people participating in the conference can form a temporary network without engaging the services of pre-existing network.[1]

Because nodes are forwarding packets for each other. some sort of routing protocol is necessary to make the routing decisions. Currently there does not exist any standard for a routing protocol for adhoc networks,instead this is work in ,progress .many problems remain to be solved before any standard can be determined. These research looks at some problems and tries to evaluate some of the currently proposed protocols.

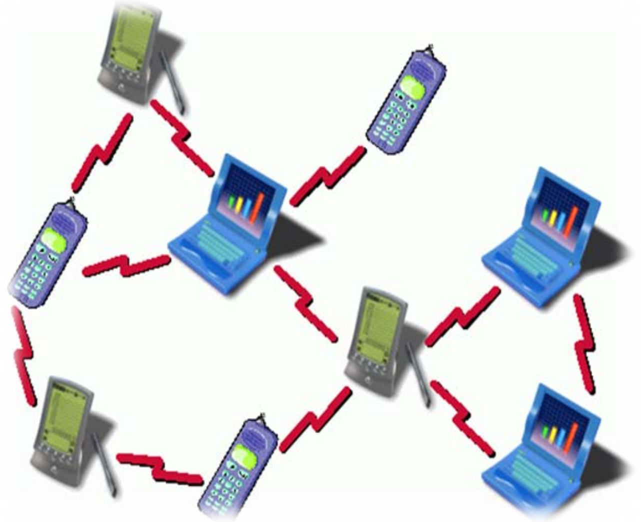

Figure1: Mobile Ad-hoc Network

A. *Problems with MANET:*

a. ***Asymmetric links:*** Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are constantly changing their position within network.

b. ***Routing Overhead:*** In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

c. ***Interference:*** This is the major problem with ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

d. ***Dynamic Topology:*** Since the topology is not constant; so the node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30sec. This updating frequency might be very low for ad-hoc networks

B. Routing:

Because of the fact that it may be necessary to hop several hops (multi-hop) before a packet reaches the destination, a routing protocol is needed. The routing protocol has two main functions, selection of routes for various source-destination pairs and the delivery of messages to their correct destination. The second function is conceptually straightforward using a variety of protocols and data structures (routing tables). This report is focused on selecting and finding routes.

C. Security:

The dynamic and cooperative nature MANET presents substantial challenges in securing these networks. Unlike wired networks which have a higher level of security for gateways and routers, ad hoc networks have the characteristics such as dynamically changing topology, weak physical protection of nodes, the absence of centralized administration, and highly dependence on inherent node cooperation. As the topology keeping changing, these networks do not have a well-defined boundary, and thus, network-based access control mechanisms such as firewalls are not directly applicable. In addition, there is no centralized detection administration, making bootstrapping of crypto systems very difficult. It is extremely easy for a malicious node to bring down the whole network. As a result, ad hoc networks are vulnerable to various attacks including eavesdropping, spoofing, modification of packets and distributed denial-of-service attacks, WormHole Attack, Rushing Attack, Blackhole Attack.

Security services, such as authentication services and access controls, can enhance the security of ad hoc networks. Nevertheless, these preventive mechanisms alone cannot deter all possible attacks (e.g., insider attackers possessing the key). Therefore, it is necessary to have other security mechanisms to deal with misbehaving insider nodes that possess the valid key and access rights. Intrusion detection, which has been successfully used in wired networks to identify attacks, can provide a second line of defense. In particular, intrusion detection and response capability is very important as many of the real ad hoc networks will be deployed in hostile environments in which legitimate nodes could be captured and used by adversaries.

Intrusion detection involves the runtime gathering of data from system operation, and the subsequent analysis of the data; the data can be audit logs generated by an operating system or packets “sniffed” from a network. [2]Intrusion detection techniques can be mapped into three concepts: signature-based detection, anomaly detection, and specification-based detection. In signature-based intrusion [3][4]detection, the data is matched against known attack characteristics, thus limiting the technique largely to known attacks, even excluding variants of known attacks.

In anomaly detection[5], profiles of normal behavior of systems, usually established through automated training, are compared with the actual activity of the system to flag any significant deviation. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, which is usually statistically significantly different from what was determined to be normal, is flagged as suspicious. Anomaly detection can detect unknown attacks, but often at the price of a high false alarm rate.

In specification-based detection,[6][7] the correct behaviors of critical objects are manually abstracted and crafted as security specifications, which are compared with the actual behavior of the objects. Intrusions, which usually cause object to behavior in an incorrect manner, can be detected without exact knowledge about them. So far, specification-based detection has been applied to privileged programs, applications, and several network protocols.

D. Type of Attacks[8]:

a. ***Spoofed, Altered, or Replayed Routing Information:*** This is the most direct attack against a routing protocol. Adversaries may be able to create routing loops, extend or shorten source routes, generate false error messages, partition the network, or increase end-to-end delay latency
b. ***Selective Forwarding:*** Malicious nodes may refuse to forward certain messages, drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a *black hole* refuses to forward every packet she sees. It is most effective when the attacker is explicitly included on the path of a data flow.
c. ***Sinkhole Attacks*:** Adversary tries to take control of all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Due to either real or imagine high quality route through compromised node, each neighboring node of the adversary will forward packets destined for a base station through the adversary. Since all packets share the same destination (the only base station), a compromised node needs only to provide a single high quality route to the base station to influence a large number of nodes
d. ***The Sybil Attack*:** In a Sybil attack[9], a single node presents multiple identities to other nodes in the network.

The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage [10], dispersity [11] and multipath [12] routing, and topology maintenance [13], [14]. This type of attack can reduce the effectiveness of fault-tolerant schemes and pose a threat to geographic routing protocols.

e. ***Wormholes :*** In the Wormhole attack, an adversary tunnels messages received one part of the network over a low latency link and replays them in a different part. Wormholes can be used to convince two distant nodes that they are neighbors by relaying packets between the two of them. These attacks can be combined with selective forwarding or eavesdropping.

f. ***HELLO Flood Attacks:*** A laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. HELLO floods can be considered as one-way broadcast wormholes and uses a single hop broadcast to transmit a message to a large number of nodes unlike the traditional definition of flooding denoting epidemic-like propagation of a message to every node in the network

II. ISSUES WITH EXISTING WORK

a. In the existing work, no initial eligibility group membership criteria is defined for a node But in this presented work, we have defined an eligibility criteria based on response time, mobility vector and throughput analysis.
b. In existing work, a symmetric criteria is defined for next hop selection in all cases. But in this proposed work, we have defined two different criteria. One, for the node within group and second for intergroup communication.
c. A weighted approach will be implemented to identify trustfulness of the nodes.

III. OBJECTIVES

a. The main objective of the work is to define a group key authentication over the mobile groups based on which the trust level of each node will be defined.
b. We will define a new parametric consideration of trustworthy next hop selection based on node existence in same group and in other group.
c. The overall objective of the work is to define a trustful route over the network that will give effective communication in case of selfish nodes as well as in congested networks.

IV. PROPOSED WORK

The presented work is the improvement over a trust aware routing over the network by performing a group key authentication along with trustworthy next hop selection over the network. The complete work is divided in three sub tasks:

A. Group Adaptability:

In this work, a node will be verified to be the part of a specific group or not. The group validity will be checked under some defined constraints. In this work we have defined three main constraints

a. Communication Range
b. Throughput Analysis
c. Response Time

The communication range is basically defined as the coverage area in terms of neighbour node selection. The communication range will selected based on the direct one to one communication basis. Based on the same parameter the transmission rate will be analyzed along with response time. A node that will provide effective and efficient throughput in defined time will be elected as the group member.

B. Group Key Authentication:

At the second phase the authentication scheme is defined under the diffie-hellman based group key approach to identify the validity of node. We have used group key based
the group will be assigned by same public key that will be verified by a group manager or the base station. The authentication will be maintained only once as the communication will begin and the session will be established. Once the session declared the route generation will be performed.

C. Route Generation:

The motive of the work is to generate a trust aware route over the network. The trustfulness of a node will be defined separately based on the route existence in a group or outside the group.

If the next hop exist in the group itself, the trust level will be analyzed by using two main parameters called

a. Response Time Analysis
b. Membership time in a group

If the node does not exist in same group the parameter depends on three main parameters

a. Response Time
b. Membership time in a group
c. Number of Overlapping Groups

V. CONCLUSION

The presented work is about to define a trustful routing over the network so that the effective communication will be performed over the network. The trustfulness of the work is defined so that the communication will be performed over the reliable nodes. The presented work will ensure the a safe and reliable communication over the mobile network so that network throughput will be improved.

VI. REFERENCES

[1]. ZhangYu," The Scheme of Public Key Infrastructure for Improving Wireless Sensor Networks Security", 978-1-4673-2008-5/12 ©2012 IEEE (pp 527-530).

[2]. Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko ,Rattapon Limprasittiporn,Jeff Rowe and Karl Levitt “A Specification-based Intrusion Detection System for AODV”, University of California, Davis {ctseng, pbala, rlim, rowe, levitt} @ucdavis.edu

[3]. K. Ilgun, R. Kemmerer, and P. Porras , “State Transition Analysis: A Rule-based Intrusion Detection Approach”, IEEE Transactions of Software Engineering, 2(13):181-199, March 1995.

[4]. U. Lindqvist and P. Porras, “Detecting Computer and Network Misuse through the Production-Based Expert System Toolset (P-BEST)”, In Proceedings of the 1999 Symposium on Security and Privacy, May 1999.

[5]. H. Javitz and A. Valdes, “The NIDES Statistical Component Description and Justification,” Technical Report, Computer Science Laboratory, SRI International, Menlo Park, CA , Mar 1994.

[6]. C. Ko, P. Brutch, J. Rowe, J., et al. 2001. System Health and Intrusion Monitoring Using a Hierarchy of Constraints. In Proceedings of the 4th Symposium on Recent Advances in Intrusion Detection. Davis, CA.

[7]. C. Ko, M. Ruschitzka and K. Levitt, “Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-based Approach,” In Proceedings of the 1997 IEEE Symposium on Security and Privacy, May 1997.

[8]. Chris Karlof and David Wagner “Secure Routing in Wireless Sensor Networks Attacks and Countermeasures”, University of California at Berkeley□ ckarlof,daw@cs.berkeley.edu

[9]. J. R. Douceur, “The Sybil Attack,” in 1st International Workshop on Peer-to-Peer Systems (IPTPS ’02), March 2002.

[10]. Castro and Liskov, “Practical byzantine fault tolerance,” in OSDI: Symposium on Operating Systems Design and Implementation. USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, 1999.

[11]. A. Banerjea, “A taxonomy of dispersity routing schemes for fault tolerant real-time channels,” in Proceedings of ECMAST, vol. 26, May 1996, pp.129–148.

[12]. K. Ishida, Y. Kakuda, and T. Kikuno, “A routing protocol for finding two node-disjoint paths in computer networks,” in Internation Conference on Network Protocols, November 1992, pp. 340–347.

[13]. Y. Xu, J. Heidemann, and D. Estrin, “Geography-informed energy conservation for ad hoc routing,” in Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2001.

[14]. B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, “Span: An energy-efficient coordination algorithm for topology maintenance in adhoc wireless networks,” ACM Wireless Networks Journal, vol. 8, no. 5,September 2002.