Sixth International Conference on Emerging trends in Engineering and Technology (ICETET'16)
www.ijera.com
ISSN: 2248-9622, pp.30-34

RESEARCH ARTICLE OPEN

Enhanced Intrusion Detection Systems For Discovering Malicious Nodes Against Collaborative Attacks

[1]A. Tharik Nazeem,[2]Y. Harold Robinson, [3]S. Divya,
[1]PG Scholar, [2]Associate Professor,[3]PG Scholar Department of Computer Science SCAD College of Engineering and Technology Tirunelveli, Tamil Nadu, India

ABSTRACT
The unique peculiarities of portable specially appointed net-lives up to expectations (Manets), including element topology and open remote medium, may lead Manets experiencing numerous security vulnerabilities. In this paper, utilizing late advances in questionable thinking started from manmade brainpower group, we propose a brought together trust administration plan that improves the security in Manets. In the proposed trust administration plot, the trust model has two parts: trust from immediate perception and trust from roundabout observation. With immediate perception from a spectator hub, the trust worth is inferred utilizing Bayesian surmising, which is a sort of unverifiable thinking when the full likelihood model can be characterized. Then again, with circuitous perception, additionally called used data that is gotten from neighbor hubs of the eyewitness hub, the trust worth is determined utilizing the Dempster-Shafer hypothesis, which is an alternate sort of unverifiable thinking when the suggestion of investment might be determined by a circuitous strategy. Joining these two parts in the trust model, we can get more correct trust values of the watched hubs in Manets. We then assess our plot under the situation of MANET steering. Broad reenactment results demonstrate the adequacy of the proposed plan. Particularly, throughput and parcel conveyance proportion can be enhanced fundamentally with somewhat expanded normal end-to-end deferral and overhead of messages.
Keywords: Time evolving topology model, Two Channel cryptography, cloud storage and data sharing.

I. 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, vehicles, and operational command centers. There are many risks in military environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless transmission medium, nomadic and distributed nature, lack of centralized infrastructure of security protection. Therefore, security in tactical MANETs is a challenging research topic There are two complementary classes of approaches that can safeguard tactical MANETs prevention-based and detection based approaches. Prevention-based approaches are studied comprehensively in MANETs. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, 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, then the whole network may be paralyzed. Furthermore, although prevention-based approaches can prevent misbehavior, there are still chances remained for malicious nodes to participate in the routing procedure and disturb proper routing establishment. It interprets trust as the degree of belief that a node performs as expected. We also recognize uncertainty in trust evaluation. Based on this interpretation, we propose a trust management scheme to enhance the security of MANETs. The difference between our scheme and existing schemes is that we use uncertain reasoning to derive trust values. On an assumption, that each party is semi-honest. In particular, a party is deemed semi-honest when the party follows the protocol properly with the exception that it keeps a record of all its intermediate computation results and then tries to deduce further information in addition to the protocol result. Moreover, researchers also assume that every party does not collude or share its record with any other party. However, since intermediate messages are exchanged between parties throughout this method, these messages may be used to deduce private information of other parties.

II. EXISTING APPROACH

Existing approaches do not carry out direct and indirect observation. The existing scheme has a very low throughput even if the number of malicious nodes is very small. The existing scheme is severely affected by malicious nodes that drop or modify packets. OLSRv2 is susceptible to various attacks such as worm hole attacks, black hole attacks, spoofing, jamming, and so on. Packet dropping attack is also called as a black hole

attack, which is a type of denial-of-service attacks. Modification of packets may have a significant impact on a topology map. The disadvantages in existing approaches are**,** Nodes with low trust values are chosen. Misbehaviors occurred such as dropping or modifying packets. It Increases average end-to-end delay.

III. THE PROPOSED SCHEME

A. Proposed Approach

We propose a unified trust management scheme which enhances the security in MANETs. In the proposed trust management scheme, the model has two components: trust from direct observation and trust from indirect observation. The proposed scheme here differentiates data packets and control packets, and excludes the other causes that result in dropping packets. The node has a good history of past experience, but it drops or modifies packets recently. In order to handle this, a windowing scheme is proposed. Compared to the proposed scheme, the existing scheme has a very low throughput even if the number of malicious nodes is very small. In this paper, our scheme is a security mechanism that mainly protects OLSRv2 against two types of misbehaviors, dropping packets and modifying packets. It improves throughput and packet delivery ratio. It decreases average end-to-end delay. Malicious nodes that deliberately drop or modify packets can be detected.

1. Problem Statement

Comparing direct observation in trust evaluation with indirect observation, indirect observation or second-hand information is important to assess the trust of observed nodes. The collection of testimonies from neighbour nodes can detect the situation where a hostile node performs perfectly to one observer, while the same performing poorly according to another node. On detection based approaches based on trust in MANETs, most of existing approaches do not exploit direct and indirect observation also called as second-hand information that is obtained from third party nodes at the same time to evaluate the trust of an observed node.

2. Return-Oriented Programming

Return-oriented programming is a technique that has evolved from stack-based buffer overflows. In ROP exploits, an attacker crafts gadgets in a sequence that are present in existing code to perform uninformed computation. A gadget is a small sequence of binary code that results in a ret instruction. By carefully crafting a sequence of addresses on the software stack, an attacker can operate the ret instruction semantics to jump to arbitrary addresses that correspond to the beginning of gadgets. This allows the attacker to perform arbitrary computation. These technique works in both word-aligned architectures like RISC and unaligned CISC architectures. ROP techniques can be used to create root kits, can inject code into Harvard architectures, and have been used to perform privilege escalation in Android. Initiating a ROP attack is made easier by the availability of architecture-independent algorithms to automate gadget creation.. Additionally, the same technique of stringing together gadgets has been adopted to control other instructions, such as jmp and their variants.

2.1 Enabling Factors For Code-Reuse Attacks

Based on our analysis of ROP attacks and defenses, we have recognized distinct characteristics and requirements for a successful exploit. The fundamental supposition and enabling factor for such attacks is as follows: The offsets of instructions in the application's code are constant. That is, if an outside attacker knows any symbol's address in the application code, then the location of all gadgets and symbols in applications codebase is deterministic. We dispute that a defensive technique that demoralizes these invariants will present a robust protection mechanism against these threats.

2.2 Preprocessing Phase

Marlin randomizes the application of binary at the granularity of function blocks. This requires identifying the function blocks in the application binary. In this, the ELF binary is parsed to extract the function symbols and allied information such as start address of the function and length of the function block. However, traditional binaries are typically stripped binaries and it has no symbol information. In such cases, we first restore the symbol information using an external tool. Once the symbol information is restored and identified, we proceed on to the next stage of Marlin processing that randomizes the application binary. It proceeded on to the next stage of Marlin processing that randomizes the application binary.

$$\lambda_i = \frac{\sum_{u,j\neq i} \pi_u(r_i) p_u(r_j|r_i)}{\sum_u \pi_u(r_i)},$$

$$\mu_i = \frac{\sum_{u,j\neq i} \pi_u(r_j) p_u(r_i|r_j)}{\sum_u (1 - \pi_u(r_i))}.$$

3. Optimization Techniques

A straight-forward performance optimization for Marlin would be to perform the pre-processing for jump patching only once for each application and store the result in a database maintained by the system. The jump patching algorithm can reuse the information about function blocks from this database in subsequent executions. The database would only need to be updated when the application code changes. The impact of the code randomization can be reduced by taking the permutation generation off-line. To do so, each application will have a dedicated file containing the next instance's permutation. When a binary is executed, the custom shell sends a signal to a trusted daemon process that runs with low priority and returns the next permutation. The application's function blocks are then shuffled accordingly.

IV. EXPERIMENTS

Creation Of Mobile Nodes

The mobile nodes in a group (i.e., cluster) cooperatively deliver data packets among each other. The key assumption here is that the mobile nodes in the same group always help each other for data delivery.

Selecting Group Of Player To Coalition Formation

The first uses a social network analysis (SNA)-based approach to identify the potential of mobile nodes which can help other mobile nodes for delivery of data in the same group or coalition. After SNA based mobile nodes grouping is done, the mobile nodes in each group play a coalitional game to obtain stable coalitional structure. This coalitional game formulation is to study how mobile nodes can dynamically form coalitions to co-operatively forward data of other mobile nodes in the same coalition. This applies social network analysis to reduce the complexity computations of coalition formation.

Establishing Coalition Procedure In Cooperative Networks

A distributed coalition formation algorithm is proposed which guarantees that stable coalitional structures can be obtained. We perform a comprehensive performance evaluation to make free transmission. The cooperative packet delivery scheme, the mobile nodes consider whether they should form a coalition, and if they form coalition which c.

The source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again.

The end-to-end delay of the CBDS for different thresholds does not increase when the number of malicious nodes increases. We further study the effect of thresholds on the end-to-end delay. Although a threshold of 85% produces the shortest delay, the resulting packet delivery ratio appears to be lower than that produced when the threshold is set to 95% or is set to the dynamic threshold value.

In Traffic Info, every time a node travels through a road segment and reaches the end of it produces a travel-time report for *s* and triggers a broadcast. The broadcast includes the produced report and the reports in database. Observe that a node may have a lot of reports to transmit in a broadcast but it may not be able to transmit all of them due to bandwidth constraints. How many reports a node can transmit in a broadcast is determined to optimize the utilization of bandwidth. Intuitively, if the transmission size is too small, then the bandwidth is underutilized and the report dissemination suffers. On the other hand, if the transmission size is too big, then many collisions would reduce the number of successfully received reports. Thus there is an *optimal transmission size* that achieves the best tradeoff between the bandwidth utilization and transmission reliability. Greedy algorithm when disseminating warning messages. This technique consists of determining the adequate selection of working modes in every possible situation. A reactive position-based routing protocol that estimates the node density on the available paths that can be used to send a message, also accounting for the direction and speed of travelling nodes in order to choose the optimal path.

V. RELATED WORK

Hierarchical key management schemes would serve well for military applications where the organization of the network is already hierarchical in nature. Most of the existing key management schemes concentrate only on network structures and key allocation algorithms, ignoring attributes of the nodes themselves. Due to the distributed and dynamic nature of MANETs, it is possible to show that there is a security benefit to be attained when the node states are considered in the process of constructing a private key generator (PKG). We propose a distributed hierarchical key management scheme in which nodes can get their keys updated either from their parent nodes or a threshold of sibling nodes. The dynamic node selection process is formulated as a stochastic problem and the proposed scheme can select the best nodes to be used as PKGs from all available ones considering their security conditions and energy states. Simulation results show that the proposed scheme can decrease network compromising probability and increase network lifetime in tactical MANETs. Most of the existing key management schemes concentrate only on network structures and key allocation algorithms, ignoring attributes of the nodes. A security benefit to be attained when the node states are considered in the process of constructing a private key generator. The priority indices can be computed offline and kept as an index table which ranks the nodes based on certain constraints.

VI. PERFORMANCE EVALUATION

In this section we evaluate the performance of the proposed scheme via computer simulation, and compare it with existing scheme. For simplicity, an ideal layer and error-free communication links are assumed. The implementation of the proposed scheme is as follows.

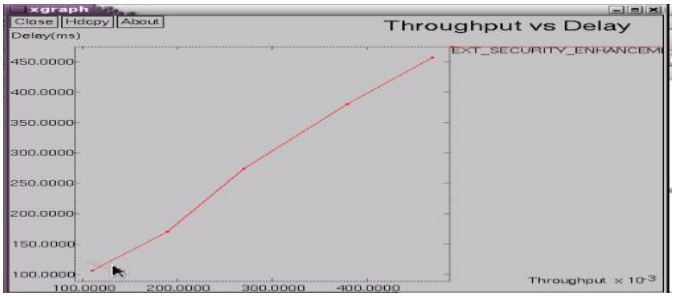

Fig: Throughput Vs Delay Graph

For relay links, based on the allocation result of the second-hop links, slots should be assigned to first-hop link with proportion to the aggregate data rate of the second-hop link of each RS. Note that the resource allocation to the first-hop link via each RS will end, when the first-hop data rate is greater than or equal to the aggregate second-hop data rate. The other slots of RZ are assigned to BS-MS.

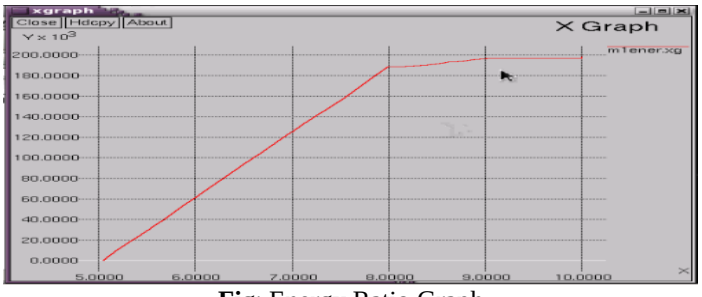

Fig: Energy Ratio Graph

The same resource in one cell can enhance the cell spectral efficiency. With regard to scheduling algorithms, MaxSINR algorithm has better spectral efficiency than RR algorithm and PF algorithm. However, there is the unfairness nature of MaxSINR algorithm. RR algorithm without considering the slot efficiency of users leads to the worst performance. We can observe that the PF algorithm offers significantly improved performance compared with the RR algorithm and takes fairness into account which MaxSINR does not. With superiority mentioned above, the PF is the most competitive scheduling algorithm for MCNs. Therefore, we adopt it as the scheduling algorithm for subsequent performance simulations.

VII. CONCLUSION AND FUTURE WORK

With recent advances in uncertain reasoning, Bayesian inference and\ Dempster-Shafer theory, we evaluate the trust values of nodes in MANETs. Misbehaviours such as dropping or modifying packets can be identified in our plan through trust standards by direct and indirect observation. Nodes with low trust values will be expelled by the routing algorithm. Therefore, secured routing path can be recognized in malicious environments. Based on the proposed scheme, more accurate trust path can be obtained by considering different types of packets, indirect observation from one-hop neighbours and other important factors such as buffers in queues and states of wireless connections, which may cause dropping packets in neighbour nodes. The results of MANET routing scenario positively support the efficiency and performance of our scheme, which improves packet delivery ratio and throughput considerably, with slightly increased average end-to-end delay with overhead of messages. In our future work, we will extend the proposed scheme to MANETs with cognitive radios

REFERENCES

[1]. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, *Member*, *IEEE*

[2]. P.-C. Tsou, J. M. Chang, H.- C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in *Proc. 2nd Intl. Conf. Wireless Commun., VITAE*, Chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[3]. S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). [Online] Available: http://www.elook.org/computing/rfc/rfc2501.html

[4]. C. Chang, Y. Wang, and H. Chao, "An efficient Mesh-based core multicast routing protocol on MANETs," *J. Internet Technol.*, Vol. 8, no. 2, pp. 229– 239, Apr. 2007

[5]. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.

[6]. I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.

[7]. A. Baadache and A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.

[8]. S.Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.

[9]. K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *Int. J. Comput. Appl.*,vol. 1, no. 22, pp. 28–32, 2010.

[10]. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[11]. H. Deng W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.

[12]. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[13]. H. Weerasinghe and H. Fu, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in *Proc. IEEE ICC*, 2007, pp. 362–367.

[14]. Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers.Commun.*, vol. 29, pp. 367– 388, 2004.

[15]. W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in *Proc. WiSec*, 2009, pp. 103–110.

[16]. W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in *Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst.*, New Delhi, India, Sep. 2009.