isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 3 ,Apr,2016 ,ISSN_NO: 2321-3337

DETECTING SELFISH NODES USING E-ACK ALGORITHM IN MANET'S

Sandhiya Rani.D.J[1] Sathika Fathi Muthu.M[2] Mrs.R.Meenakshi.M.E(Phd)
Department of Information Technology
Valliammai Engineering College Kancheepuram Dt India
Asst.Prof Sel.grade&HOD I/C *Department of Information Technology India*

Abstract- **A MANET is a peer-to-peer multi hop mobile wireless network that has neither a fixed infrastructure nor a central server some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes. The mobility and resource constraints of mobile nodes may lead to network partitioning or performance degradation. Several data replication techniques have been proposed to minimize performance degradation. Most of them assume that all mobile nodes collaborate fully in terms of sharing their memory space. Malicious nodes are hard to detect using watchdogs, as they can intentionally participates in network communication with the only goal to hide their behavior from the network. In paper, we develop a collaborative contact-based watchdog (CoCoWa) detection algorithm that considers partial selfishness and novel replica allocation techniques to properly cope with selfish replica allocation. In this project,we define solid privacy requirements regarding malicious attackers in MANET. Then we propose and implement a new intrusion-detection system named Enhanced Adaptive ACK specially designed for MANET's. E-ACK demonstrates higher malicious-behaviour detection rates in certain circumstances while does not greatly affect the net work performance.**

1.INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid development of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network

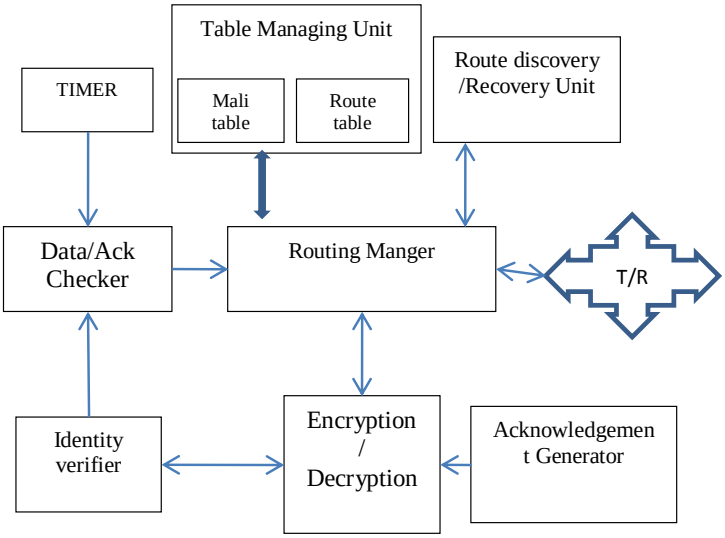
Volume: 4, Issue: 3,Special Issue: 3 ,Apr,2016 ,ISSN_NO: 2321-3337

activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delievering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path from a source to destination in a static network is usually the optimal route, this idea is not easily extended to MANETs factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power extended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network. An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self re-configuring multi hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in a multi hop forwarding. The nodes in the network not only act as hosts but also routers that route data to/from other nodes in network. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data to other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes. MANETs rely on wireless transmission, a secured way of message transmission is important to preotect the privacy of data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile adhoc networks there is no central administration to take care of detection and precention of anomalies. Mobile devices identifies or their intensions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. In ad hoc networks devices (also

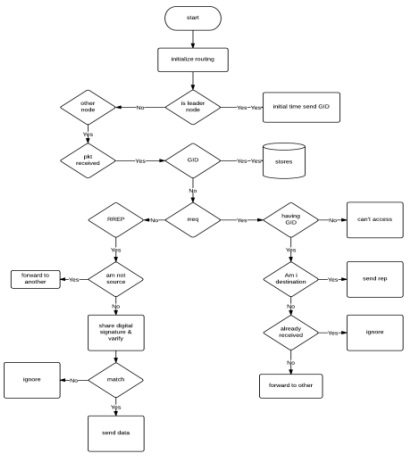
called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures. The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today. Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into internal attacks and external attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are actually authorized nodes and part of the network hence it is difficult to identify. In the next generation of wireless communication systems, there will be a need for the rapid development of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over realtively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delievering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path from a source to a destination in a static network is usually the optimal route, this idea os not easily extended to MANETs factors such as variable wireless link quality, propogation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing in the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

Volume: 4, Issue: 3,Special Issue: 3 ,Apr,2016 ,ISSN_NO: 2321-3337

2. ARCHITECTURE OVERVIEW



We have created our architecture with number of blocks, in that the work of Routing manager is used to control all the block and routing manger will desire the packet forwarding directions, and the time used to generate the time interval to generate the time interval, in that triggered time the node will check the count of ack and data by Data/Ack checker. The node can receive / Transfer the data by T/R. If the data received in node then the node has to generate the ack, the ack generation is going to be done by the ack generator. If the ack generated then that should contain the digital signing information. The digital sign info created by the Encryption/Decryption unit. If ack received then the node has to verify the ack was generated by the authorized node, this operation will be done by the Identity verifier. The Table managing unit contains the information of malicious node and route information, the route discovery and recovery unit used to construct or reconstruct the path.



At initial time the leader node will share the group id details to all other node, after receiving the GID information the node should store the information of GID in data base for future use, then if the node wants to make communication it has to search the route by the REQ, the source node will send the req to all the neighbor node. If the neighbors receive the packet then it has to very by the packet with group id and digital sign then the node will check the information such that the node is the final destination. If the node is the final destination then the node has to send reply or else the packet can forward further to the next level node. if any node received the reply, the node can update the route info after verification. If received node is the final destination for the packet then the node can ignore the packet after verification. Then the data can be transfer through the update route.

3. RELATED WORK:

There are two main strategies to deal with selfish behavior in cooperative networks. The first approach tries to motivate the nodes to actively participate in the forwarding activities. The COMMIT Protocol combines game-theoretic techniques to achieve truthfulness and an incentivation payment scheme to reduce the impact of selfish nodes on routing protocols. Regarding the detection and exclusion approach, there are several solutions for MANETs and DTNs. A first study about misbehaving nodes and how watchdogs can be used to detect them was introduced.Here we proposed a Watchdog and Pathrater over the DSR protocol to detect non-forwarding nodes, maintaining a rating for every node. In another scheme for detecting selfish nodes based on context aware information was proposed. In this approach if a node locally detects an intrusion with strong evidence, it can initiate a response. However, if a node detects an anomaly with weak evidence, it can initiate a cooperative global intrusion detection procedure. A similar approach is presented in that shows the effect of socially selfish behaviour. Social selfishness is an extension of classical selfishness (also called individual selfishness). A social selfish node can cooperate with other nodes of the same group, and it does not cooperate with other nodes outside the group. The impact of social selfishness on routing in DTN. The problem, as shown in the evaluation sections, is that if a false positive is generated it can spread this wrong information very quickly on the network, isolating nodes that are not selfish. Therefore, an approach that includes the diffusion of negative detections as well becomes necessary. Another problem is the impact of colluding or malicious nodes. In our earlier work secure transmission of the provenance requires several distinct packet transmissions. The underlying assumption is that provenance remains the same for at least a flow of packets. The basic idea in these works is to encode the link identifiers constituent to the packet routing path into an iBF. However, the encoding of the whole path is performed by the data source, whereas the intermediate routers check their membership in the iBF and forward the packet further based on this decision. This approach is infeasible for sensor networks where the paths may change due to several reasons. Moreover, an intermediate router only checks its own membership which may leave several integrity attacks such as all-one attack, random bit flips, etc., undetected. Our approach resolves these issues by encoding the provenance in a distributed fashion. Several counter selective forwarding attacks has been proposed to efficiently detect the forwarding misbehaviors of malicious nodes in battery powered WSNs.The basic idea is that a set of intermediate nodes located along a forwarding path to a sink acts as a checkpoint node to monitor any forwarding misbehavior by replying an acknowledgment (*Ack*) packet to a source node. If an intermediate node does not receive the required number of *Ack* packets within a timeout period, it suspects a malicious node and send an *Alarm* packet to the source node through multi-hop relays. The number of *Ack* packets generated from intermediate

nodes and how many *Ack* packets received by checkpoint nodes incur a performance tradeoff between detection accuracy and communication overhead. Multipath routing can be utilized to lessen the probability of encountering a malicious node. Braided paths originally designed for resiliency to node failures, create partially disjoint paths. Note that either forwarding *Ack* and *Alarm* packets via multi-hop relays or creating disjointed paths from nodes to a sink deployed in prior approaches may not directly be applicable to energy harvesting WSNs, where nodes are not always available due to energy availability. Unfortunately counter selective forwarding attacks are under-explored in energy harvesting WSNs.

4. EXISTING WORK:

A number of secure routing schemes have been brought forward for intrusion-detection in MANETs.1.WATCHDOG: It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. It will improve the throughput of network with the presence of malicious nodes.2.TWOACK: In order to overcome the drawbacks in watchdog, a new scheme is proposed that is TWOACK, to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. 3.AACK: It is similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). It can significantly reduce overhead when compared with TWOACK. Disadvantages: Existing schemes are largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic but they suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets. Another drawback of most previous schemes is the significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such overhead can easily degrade the life span of the entire network.

5.PROPOSED WORK:

In this project, we propose and implement a new and efficient intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.In the proposed method we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.Advantages: Our proposed approach EAACK completely overcomes the weaknesses like false misbehavior, limited transmission power, and receiver collision. All acknowledgment packets in EAACK are authentic and untainted.Our proposed method can significantly improve the packet delivery ratio.

6.CONCLUSION:

This paper proposes CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, false negatives and malicious nodes. CoCoWa is based on the diffusion of the known positive and negative detections. When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections. Analytical and experimental results show that CoCoWa can reduce the overall detection time with respect to the original detection time when no collaboration scheme issued, with a reduced overhead (message cost). This reduction is very significant, ranging from 20 percent for very low degree of collaboration to 99 percent for higher degrees of collaboration. In short, the combined effect of collaboration and reputation of our approach can reduce the detection time while increasing the global accuracy using a moderate local precision watchdog. In future work, we plan to implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

7. REFERENCES:

[1] Enrique Hern_andez-Orallo,Manuel David Serrat Olmos, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, **" A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes"** IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 6, JUNE 2015.

[2]" Sunho Lim† and Lauren Huie§"**Hop-by-Hop Cooperative Detection of Selective Forwarding Attacks in Energy Harvesting Wireless Sensor Networks"** 2015 International Conference on Computing, Networking and Communications (ICNC), Workshop on Computing, Networking and Communications (CNC),

[3] Salmin Sultana, Gabriel Ghinita, Elisa Bertino**," A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks"** IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3,May/June 2015.

4] Nan Kang**, "Detecting ForgedAcknowledgements in MANETs"** IEEE on Advanced Information Networking and Applications 2011

[5] Jeemi Sinha**" Identification of Trusted Nodes in Mobile Adhoc Network"** International Journal of Science and Research (IJSR) 2014

Volume: 4, Issue: 3,Special Issue: 3 ,Apr,2016 ,ISSN_NO: 2321-3337