Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 8; April-June, 2015 pp. 82-85

http://www.krishisanskriti.org/acsit.html

Checkpointing and Trust based Recovery in MANET: A Survey

Ravneet Kaur[1] and Neeraj Sharma[2]

[1]Deptt. of Computer Science and Engineering Chandigarh Engineering College Landran, Mohali, India
[2]Head of Department (CSE) Chandigarh Engineering College Landran, Mohali, India
E-mail: 1brarravneetkaur@yahoo.in, 2csem.csehod@gmail.com

Abstract—*Trust in MANET is an important concept as the nodes are mobile and can be easily prone to various attacks. The challenge lies in developing various models for the calculation of trust. Various models for trust calculations has been proposed over time and their merits and demerits have been discussed. The next challenge is to utilize that trust value for making the system robust against various attacks. The idea is to save the check-pointing data of each node to some trusted node whenever it is suspected that the node could be attacked and loose its data. Another problem with this approach is the increased overhead due to storage of this check-pointing data. Various researchers have tried to propose criterions for check-pointing and analyzed. This paper presents a comprehensive review of the various techniques and the advantages and challenges of those techniques. Finally the paper concludes with a brief discussion on the grey areas on this topic which can be explored further in future.*

1. INTRODUCTION

MANET is an ad hoc network that has no fixed infrastructure, consists of mobile nodes that move around freely and are limited by short range as well as restricted energy levels. MANETs are usually deployed in severe uncontrolled environments, thereby heightening the probability of compromises and malfunctioning as there is no centralized control unit to monitor the node operations [6]. The nodes in MANET together make up a cluster in several respects which overall can be viewed as a single system with similar nodes. Every node in a cluster is in close proximity to each other. Each cluster has a designated cluster head, gateway node and ordinary nodes [11]. Cluster head is responsible for all the communications within the cluster as well as with the neighboring clusters. Cluster members send data to the cluster head which further sends it to other cluster heads. The receiver cluster head sends the packet to the desired location. Gateway is responsible for the forwarding of the packets between two adjacent clusters. Ordinary nodes are all other nodes except the cluster head and gateway node. Cluster head and gateways are always selected with extreme care because these are the nodes that represent a cluster and are halfway between the two communicators. Basically a node with greater trustworthiness is chosen as a cluster head and the node next in the stand as a gateway node. Trust is the confidence of a node that it is able withstand for a longer time period as compared to other nodes nearer to it in space. It is a belief that the node is reliable and is able to perform efficiently in terms of energy and is fault tolerant. Usually trust factor of a node is calculated based on several factors. Many implementations have considered diverse circumstances to determine its value. In MANET, when a node moves from one cluster to another, it saves its checkpoint consisting of current process state in the cluster head and enters into new cluster. Each time it enters a new cluster, cluster_change_count is updated thereby keeping a record of the inter-cluster movements gone through [8]. When this count go beyond a predefined value, the node list down the process state in itself too i.e, it saves the checkpoint individually. In case the mobile node fails before saving its checkpoint in the new cluster then it needs to retrieve its checkpoint previously stored on one of the preceding nodes. This is a confidential matter where the sensitive information is restored back through some trusted nodes only. So trust value should be calculated considering several important factors that affect the reliability of a node.

2. LITERATURE REVIEW

In order to ensure that the system continues to operate properly in case of failures or fault in any of its components, Suparna Biswas et al. [8] proposed fault-tolerance scheme based on checkpoints and trusted nodes in which each mobile host keeps a track of the number of clusters it travels and saves its value in „cluster_change_count" every time it enters into a new cluster. If this value exceeds a specified threshold then mobile host saves the checkpoint on its own too. Now there may be a chance that the mobile host is unable to save checkpoint and fails then quick retrieval of last saved checkpoint is required which is done by transmission of checkpoint through intermediate nodes that are completely trusted and such trusted nodes are verified based on several factors like: availability, failure rate, available battery power and recommendations from other nodes. So the proposed work can be summarized as:

- Trusted nodes act as cluster heads and gateways.

- Mobile hosts saves checkpoints on its own depending upon the value of cluster_change_count.
- In case of mobile host failure, checkpoints are recovered through trusted nodes only.
- Trust value of a node is calculated based on 4 factors: availability, failure rate, energy of a node and recommendation from other nodes.

Suparna Biswas et al. [9] proposed another trust model for secure recovery of checkpoints from the last saved checkpoint node to the failed node without any requirement of encryption of data by transferring it only through trusted nodes. Encryption of checkpoints used for maintaining security can be ignored if the checkpoints are forwarded through trusted nodes only thereby reducing additional overheads associated with encryption process, reduced recovery time and reduced resource consumption. „*Reference nodes*" are the intermediate nodes used for forwarding the checkpoint from the backup node" to the „recovery node". So checkpoint is basically passed on through reference nodes that are trusted. In case, a reference node is distrusted then encryption is done and the next node on the path transfer encrypted checkpoint through the rest of the path without requiring the path nodes to calculate the trust factor again. On receiving encrypted checkpoint, the failed mobile host decrypts it using a private key. A Reference node is considered to be trusted based on its failure rate, unused battery power and security attack rate. Security attack rate is the measure of a node likely to be attacked by some other malicious node. As the maliciousness increases security attack rate increases directly.

Although encryption method is a useful approach to protect the checkpoints [9] but it is also incorporated with additional overheads thereby decreasing overall efficiency of a network. So rather than acquiring encryption technique it is far better to forward checkpoint through trusted nodes.

With the same perspective Suparna Biswas et al. [10] proposed ant colony optimization for trusted checkpointing based on ant foraging technique used by ants to spread pheromone along the path they travel to let other ants know about the shortest path leading to their food. The other ants follow the path with high pheromone density. Similarly in MANET, nodes acts as ants and pre-examining of path is done by sending a dummy packet and for each successful response pheromone list is updated. In which path for forwarding the checkpoint is selected based on trust value and Pheromone value and number of nodes along the path. Pheromone list is created using following series of steps:

- First the sender node appends the calculated hash value of the dummy packet and along with node ID of cluster members that are at 1-hop distance, sends the dummy packet to the receiver node.
- Receiver node sends acknowledgement packet to the sender on receiving dummy packet along with the same hash value. The sender node checks the attached hash value with the previous hash value. If the hash value matches: successful response; if the hash value does not match: unsuccessful response.
- If sender gets no acknowledgement packet, then the receiver node is designated as „selfish" node.
- For each successful match, the path is added on to the pheromone list.
- The nodes" ID that exists within 1-hop distance of the receiver node does not receive any dummy packet.

High pheromone quantity along the path, high probability of being selected as the checkpoint carrying path

Thus, ant colony optimization technique proposed by Suparna Biswas et at. [10] is different from the existing techniques uniquely based on pheromone calculation and also does not incorporates encryption overheads.

Asynchronous checkpointing and optimistic message logging for mobile ad hoc networks was proposed by Ruchi Tuli and Parveen Kumar [4]. They introduced not only the checkpointing scheme used for recovery but also proposed a message logging scheme in which each cluster head maintains a record of nodes available in its cluster area. Message logging at the cluster head is done to prevent the data maintenance overhead at the mobile hosts. Instead, they are responsible to hold minimum possible information because of their limited storage. Cluster head, on the other hand, keeps: Log of current nodes available in the cluster area and Log of mobility of the nodes such as which node has joined, left or disconnected the cluster. Checkpointing of nodes is also asynchronous in nature i.e., mobile host is free to make its decision regarding inclusion or exclusion from the cluster by sending reconnect" or „disconnect" messages respectively. It can independently hold its checkpoint and can move whenever it wishes to.

An approach called Access-Pattern Aware Checkpointing Data Storage Scheme has been proposed by Xiang Li et. al. [13] based upon the „sojourn time" (basically lapse time of a node within MSS, Mobile Support Stations). This time reflects the usage of a node and depends on „visit rate" of a node which is the rate at which mobile host visit MSS. Its value is dependent on visit frequency and time. Threshold of visit rate is calculated and during handoff (transition from one base station to another) if visit rate exceeds its threshold then successful recovery is possible as the required log and checkpoints are transferred to the new MSS from the previous MSS. Conversely, if threshold is greater than visit rate then there is very little scope of recovery. Greater stay time within MSS, greater the probability of successful recovery. Thus, recovery is directly based on the only factor, visit rate. Comparison with existing schemes such as pessimistic approach, eager and lazy schemes has been made where the proposed access pattern scheme depicts more flexible performance.

Awadesh Kumar et. al. proposed message log unifying and movement based checkpointing scheme for asynchronous rollback recovery in cluster based multi hop mobile ad hoc networks [5]. In this virtual region is envisaged as the region consisting of the current cluster head and its neighbors. The current cluster head is called as CMC (Checkpoint and Movement Coordinator). Checkpoints are taken based on the movement of mobile host i.e, as long as the mobile host is within the virtual region no checkpoints are taken and as it moves next to the neighbors of the CMC, checkpoint is taken at the new cluster head and it becomes the new CMC. So, in case of failures, the recovery procedure collects recovery related data from the CMC or at-most two CHs (referred to as recovery set). The proposed scheme employs message log unifying scheme in which the message log is periodically updated at the CMC. When a MH fails outside the virtual region, message log unified at the CMC and the most recent checkpoint are sent to the current CH of the MH where it failed. It is advantageous in the sense that multiple MHs can collect recovery information simultaneously. Also, self-stabilizing spanning tree is engaged in the work which builds a legitimate spanning tree of the available CHs, when there is change in the topology of the CHs (leaves or joins). The recommended work results into decreased number of recovery messages contrary to high number in flooding. Again, the number of recovery messages decreases with increase in number of clusters because then the probability of MH within the virtual region increases and no checkpointng is required there.

One more approach announced by Poonam Gera et. al. [2] for enhancing data security in MANETs is a multi-path routing scheme in which the confidential data to be sent is broken up into smaller modules and pairs of them are sent along the multiple paths and that too are self-encrypted using simple XOR operation. Thus, computation is minimized as no encryption and decryption keys are required. A trusted path is found out which has trust greater than a specified threshold and this path, referred to as indicator path, carries the message pair information. Destination node, on receipt of individual data parts from the different passages, sorts them down based on unique identifier provided to each part. Trust value among nodes of the multiple trust paths is calculated based on mutual trust among the nodes. Misbehaving nodes that may act as attacker nodes are ignored based on their trust value. Thus, the proposed work provides secure communication during two phases: routing phase, where disjoint paths (each path with different unique nodes) are selected to transfer fragmented data; misbehaving nodes ignored and second is transmission phase, where secure transmission is made between the two ends using self-encryption of individual data parts. Fragmented data is sent along different paths, and further encryption is done leading to difficult access. For an attacker, this becomes troublesome job to be done to get the whole data. Although much secure connection is established but lots of calculations and the encryption process makes it inconvenient to operate practically.

Trust Aware Routing Framework is implemented along with Link Failure Consideration by Prashant P. Rewagad and Satish R. Suryawanshi [1]. They integrated the existing TARF (Trust Aware Routing Framework) and BLME (Backup Link Mutual Exclusion) techniques so as to make the existing structure more robust. TARF provides efficient routing considering the trust factor and energy of the nodes.

Summary Vector Table", consisting node"s neighbor information in terms of trust and energy, is periodically updated. Trust factor is calculated from the occurrence of network loops and delivery ratio. TARF approach specifically protects against identity impersonation attacks. BLME technique is used to recover from dual link failures without the need for broadcasting the failure location to all nodes [3] and provides backup path for any failed link. When two simultaneous link failures occur BLME ensures that same path is not used as backup by both failed links. Also, backup paths are not created until and unless link failure occurs, otherwise it may require additional computations. The above methodology results into minimum delay and packet loss.

Jing-Wei Huang et. al. [14] proposed trust based multipath AOMDV protocol integrated with encryption process. Fragmented message parts are encrypted using bit operation XOR and are routed through multiple paths to reach the destination where these individual parts are decrypted at the sink. The proposed scheme is different from the existings ones such that it uses „degree of secrecy" to find an appropriate path for transfering the fragmented message modules. Least trusted node in a path is recognised as the path trust value and for a higher path trust value, degree of secrecy is higher. For a lower number, secrecy mark gets lowered. Thus, data is transferred on to the path which has the same secrecy degree as the one pre-defined for the data i.e., the data and the path"s degree must be consistent with each other.

Trust value increases or decreases based on successful transmission of data packets by a node and this value is determined by its neighboring nodes with which the node communicates thus, classifying nodes into two categories: well-behaved and malicious. The proposed T-AOMDV (Trust - Ad Hoc On-Demand Multipath Distance Vector) protocol quickly selects better routes by finding trusted node-disjoint paths when compared to the existing T-DSR scheme, where the latter fails to do so.

3. CONCLUSION

In this paper, review of some important aspects of recovery in clusters has been done. It is observed that trust value of a node is a crucial factor that considerably contributes towards successful recovery of checkpoints in case of node failures. Various approaches discussed above determine the trust value based on several factors that directly or indirectly constitute an overall trust value of a cluster. We surveyed that if only trusted nodes are used as halfway between the two ends for checkpoint transmission, low recovery time as well as better

efficiency of the network, are the outcomes. Some approaches are directed towards reducing the number of checkpoints, so that the recovery messages are reduced and thus, the overhead. Few others aimed to retrieve checkpoints through multiple paths. Related literature work is presented above. Thus, different trust algorithms are devised keeping in view various facts regarding cluster nodes such as their mobility, energy, failure rate, etc. Above all, the prime objective to make the recovery process shorter and simpler is achieved using several trust mechanisms for secure communication.

4. FUTURE SCOPE

So far, the means to determine trust factor are sparse and are limited to few aspects only. It lacks absoluteness. Social influence on nodes is one such feature which can be researched intensively. It can be added on with the existing features. Moreover, dynamic recovery of failed nodes can be emphasized. So, we hope that we would be able to bring up more stronger and more secure mobile network very soon in the near future which would be a blend of some existing aspects and few recommendations that need keen investigation.

REFERENCES

[1] Prashant P. Rewagad and Satish R. Suryawanshi, "Implementation of Trust Aware Routing Framework With Link Failure Consideration and Recovery", *International Journal of Research in Computer and Communication Technology, Vol 3, Issue 9, September – 2014.*

[2] Poonam Gera, Kumkum Garg, and Manoj Misra, "Trust-based Multi-Path Routing for Enhancing Data Security in MANETs", *International Journal of Network Security, Vol.16, No.2, PP.102-111, Mar. 2014.*

[3] C. M. Jadhav, Amruta. R. Shegadar, S. Shabade, "Dual-Link Failure Resiliency through Backup Link Mutual Exclusion", *International Journal Of Engineering And Computer Science, ISSN:2319-7242 Volume 3 Issue, 12 December 2014.*

[4] Ruchi Tuli and Parveen Kumar, "Asynchronous Checkpointing and Optimistic Message Logging for Mobile Ad Hoc Networks", *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 10, 2011.*

[5] Awadhesh Kumar Singh and Parmeet Kaur Jaggi, "Asynchronous Rollback Recovery in Cluster Based Multi Hop Mobile Ad Hoc Networks", *International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471, Vol. 2 Issue 6, June-2013*

[6] Kannan Govindan and Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", *IEEE.*

[7] Renu Dalal, Manju Khari and Yudhvir Singh, "Different Ways to Achieve Trust in MANET", *International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.*

[8] Suparna Biswas, Sarmistha Neogy and Priyanka Dey, "Mobility based checkpointing and trust based recovery in MANET", *International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 4, August 2012.*

[9] Suparna Biswas1, Priyanka Dey and Sarmistha Neogy, "Secure Checkpointing-Recovery using Trusted Nodes in MANET", *4th International Conference on Computer and Communication Technology (ICCCT), 2013.*

[10] Suparna Biswas1, Priyanka Dey and Sarmistha Neogy, "Trusted Checkpointing Based on Ant Colony Optimization in MANET", *Third International Conference on Emerging Applications of Information Technology (EAIT), 2012.*

[11] RuchiTuli and Parveen Kumar, "Minimum process coordinated checkpointing scheme for ad hoc networks", *International Journal on AdHoc Networking Systems (IJANS) Vol. 1, No. 2, October 2011.*

[12] Pooja Sharma & Dr. Ajay Khunteta, "A Survey of Checkpointing Algorithms in Mobile Ad HocNetwork", *Global Journal of Computer Science and Technology Network, Web & Security, (USA), Volume 12 Issue 12 Version 1.0 Year 2012.*

[13] Xiang Li, Mei Yang, ChaoGuang Men, YingTao Jiang and Kalum Udagepola, "Access-Pattern Aware Checkpointing Data Storage Scheme for Mobile Computing Environment", *Procedia Computer Science, 34 (2014) 330 – 337, Elsevier, 2014.*

[14] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi and Sanjay K. Dhurandher, "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", *IEEE Globecom 2011.*