Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.947 – 953

RESEARCH ARTICLE

SECURE AND EFFICIENT ROLLBACK RECOVERY IN GRID ENVIRONMENT

Ms. A. Wisy Shantha
PG Scholar of CSE Department
R.V.S Faculty of Engineering, Coimbatore
India
wisyabraham22@gmail.com

Prof. S. Subashini
Assistant Professor of CSE Department
R.V.S Faculty of Engineering, Coimbatore
India
deancsefoe@rvsgroup.com

Abstract— Large applications executing on Grid or cluster architectures consisting of hundreds or thousands of computational nodes create problems with respect to reliability. The source of the problems is node failures and the need for dynamic configuration over extensive runtime. This paper presents two fault-tolerance mechanisms called Theft-Induced Check pointing and Systematic Event Logging. These are transparent protocols capable of overcoming problems associated with both benign faults, i.e., crash faults, and node or subnet volatility. Specifically, the protocols base the state of the execution on a dataflow graph, allowing for efficient recovery in dynamic heterogeneous systems as well as multithreaded applications. By allowing recovery even under different numbers of processors, the approaches are especially suitable for applications with a need for adaptive or reactionary configuration control. The low-cost protocols offer the capability of controlling or bounding the overhead. A formal cost model is presented, followed by an experimental evaluation. It is shown that the overhead of the protocol is very small, and the maximum work lost by a crashed process is small and bounded. One possible solution to address heterogeneity is to use platform independent abstractions such as the Java Virtual Machine. However, this does not solve the problem in general. There is a large base of existing applications that have been developed in other languages. Reengineering may not be feasible due to performance or cost reasons. Environments like Microsoft .Net address portability but only few scientific applications on Grids or clusters exist.

I. INTRODUCTION

The self-generated and forwarded packets by a node are passed to the decrease and increase the node's credit account, respectively. Packet purse and packet trade models have been proposed. For the packet purse model, the source node's credit account is charged the full payment before sending a packet, and each intermediate node acquires the payment for relaying the packet. For the packet trade model, each intermediate node runs an auction to sell the packets to the next node in the route, and the destination node pays the total cost of relaying the packets. After receiving a data packet, the destination node sends a RECEIPT packet to the source node to issue a REWARD packet to increment the credit accounts of the intermediate nodes. In CASHnet, the credit account of the source node is charged and a signature is attached to each data packet. Upon receiving the packet, the credit account of the destination node is also charged,

and a digitally signed acknowledgement (ACK) packet is sent back to the source node to increase the credit accounts of the intermediate nodes.

The receipt-based payment schemes impose more overhead than the TPD-based schemes because they require submitting receipts to the AC and processing them. However, the TPD-based payment schemes suffer from the following serious issues. First, the assumption that the TPD cannot be tampered with, cannot be guaranteed because the nodes are autonomous and self-interested, and the attackers can communicate freely in an undetectable way if they could compromise the TPDs. Second, the nodes cannot communicate if they do not have sufficient credits during the communication time. Unfortunately, the nodes at the network border cannot earn as many credits as the other nodes because they are less frequently selected by the routing protocol. Finally, since credits are cleared in real time, the multihop communications fail if the network does not have enough credits circulating around because the nodes do not have sufficient credits to communicate. In is shown that the overall credits in the network decline gradually with using TPD-based schemes because the total charges may be more than the total rewards. This is because the source node is fully charged after sending a packet but some intermediate nodes may not be rewarded when the route is broken.

In order to eliminate the need for TPDs, an offline central bank called the AC is used to store and manage the nodes' credit accounts. In Sprite, for each message, the source node signs the identities of the nodes in the route and the message, and sends the signature as a proof for sending a message. The intermediate nodes verify the signature, compose receipts containing the identities of the nodes in the route and the source node's signature, and submit the receipts to the AC to claim the payment. The AC verifies the source node's signature to make sure that the payment is correct. However, the receipts overwhelm the network because the scheme generates a receipt per message. Unlike Sprite that charges only the source node, FESCIM adopts fair charging policy by charging both the source and destination nodes when both of them are interested in the communication. In PIS, the source node attaches a signature to each message and the destination node replies with a signed ACK packet. PIS can reduce the receipts' number by generating a fixed-size receipt per session regardless of the number of messages instead of generating a receipt per message in Sprite. In order to reduce the communication and processing overhead, CDS uses statistical methods to identify the cheating nodes that submit incorrect payment. However, due to the nature of the statistical methods, the colluding nodes may manage to steal credits, and some honest nodes may be falsely accused of cheating which is called false accusations. Moreover, some cheating nodes may not be identified which is called missed detections, and it may take long time to identify the cheating nodes.

II. RELATED WORKS

In recent years, mobile ad hoc networks have received much attention due to their potential applications and the proliferation of mobile devices. Specifically, mobile ad hoc networks refer to wireless multi-hop networks formed by a set of mobile nodes without relying on a preexisting infrastructure. In order to make an ad hoc network functional, the nodes are assumed to follow a self-organizing protocol, and the intermediate nodes are expected to relay messages between two distant nodes. Recent evaluations have shown that ad hoc networks not only are flexible and robust, but also can have good performance in terms of throughput; delay and power efficiency [1].

Mobile ad hoc networking has been an active research area for several years. How to stimulate cooperation among selfish mobile nodes, however, is not well addressed yet. In this project, a simple, cheat-proof, credit based system for stimulating cooperation among selfish nodes in mobile ad hoc networks. The system provides incentive for mobile nodes to cooperate and report actions honestly. Compared with previous approaches, the system does not require any tamperproof hardware at any node [1]. Furthermore, a formal model of the system and prove its properties. Evaluations of a prototype implementation show that the overhead of the system is small. Simulations and analysis show that mobile nodes can cooperate and forward each other's messages, unless the resource of each node is extremely low.

A new system is proposed called TACS, trusted and attacker free credit based scheme for wireless networks. It is for stimulate node co-operation, avoid packet drop, and regulate packet transmission. The node submits report to the trusted party after the communication is over and store a temporarily undeniable token called evidences. The trusted party verifies the report and clears the payment of fair report with no processing overhead. For cheating reports evidences are requested to identify and remove cheating node from the system. In the new system all the attacker nodes are removed before beginning the communication and a trust value is assigned to all the nodes. This will improve the security of the system and it has low communication overhead, processing overhead [1].

A computer network is a telecommunications network that connects a collection of computers to allow communication and data exchange between systems, software applications, and users. The computers that are involved in the network that originate, route and terminate the data are called nodes. The interconnection of computers is accomplished with a combination of cable or wireless media and networking hardware. Multihop Wireless Network (MWN): A wireless network adopting multihop wireless technology without deployment of wired backhaul links. It is similar to Mobile Ad hoc Networks (MANET), Nodes in the MWN is relative fixed [2].

Mobile ad-hoc network is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. A wireless network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity [2].

For example users in a college campus having different wireless devices such as cell phones, laptops etc in order to share information and distribute files the can establish a communication. The assumption is that each node willing to share its resources such as clock cycles, bandwidth etc. There are selfish nodes the doesn't relay others packet and uses cooperative nodes to relay their own packets, this causes performance degradation and failing of multihop networks. To avoid this a payment scheme is introduced such that when a node relays forwarded packet the get a credit and that credit can be used for forwarding self generated packet also [3].

In military and rescue applications of mobile ad hoc networks, all the nodes belong to the same authority; therefore, the are motivated to cooperate in order to support the basic functions of the network. The case when each node is its own authority and tries to maximize the benefits it gets from the network. More precisely, assume that the nodes are not willing to forward packets for the benefit of other nodes. This

problem may arise in civilian applications of mobile ad hoc networks. In order to stimulate the nodes for packet forwarding, a simple mechanism based on a counter in each node. The behavior of the proposed mechanism analytically and by means of simulations, and detail the way in which it could be protected against misuse [3].

A mobile ad hoc network is a wireless multi-hop network formed by a set of mobile nodes in a self organizing way without relying on any established infrastructure. Due to the absence of infrastructure, all networking functions must be performed by the nodes themselves. For instance, packets sent between two distant nodes are expected to be forwarded by intermediate nodes. This operating principle of mobile ad hoc networks renders cooperation among nodes an essential requirement. By cooperation, at the nodes perform networking functions for the benefit of other nodes. As pointed out, lack of cooperation may have fatal effects on network performance. So far, applications of mobile ad hoc networks have been envisioned mainly for crisis situations (e.g., in the battlefield or in rescue operations). In these applications, all the nodes of the network belong to a single authority (e.g., a single military unit or rescue team) and have a common goal. For this reason, the nodes are naturally motivated to cooperate. However, with the progress of technology, it will soon be possible to deploy mobile ad hoc networks for civilian applications as well. Examples include networks of cars and provision of communication facilities in remote areas [5].

III. RACE

As shown in Fig. 2, RACE has four main phases. In Communication phase, the nodes are involved in communication sessions and Evidences and payment reports are composed and temporarily stored. The nodes accumulate the payment reports and submit them in batch to the TP. For the Classifier phase, the TP classifies the reports into fair and cheating. For the Identifying Cheaters phase, the TP requests the Evidences from the nodes that are involved in cheating reports to identify the cheating nodes. The cheating nodes are evicted and the payment reports are corrected.

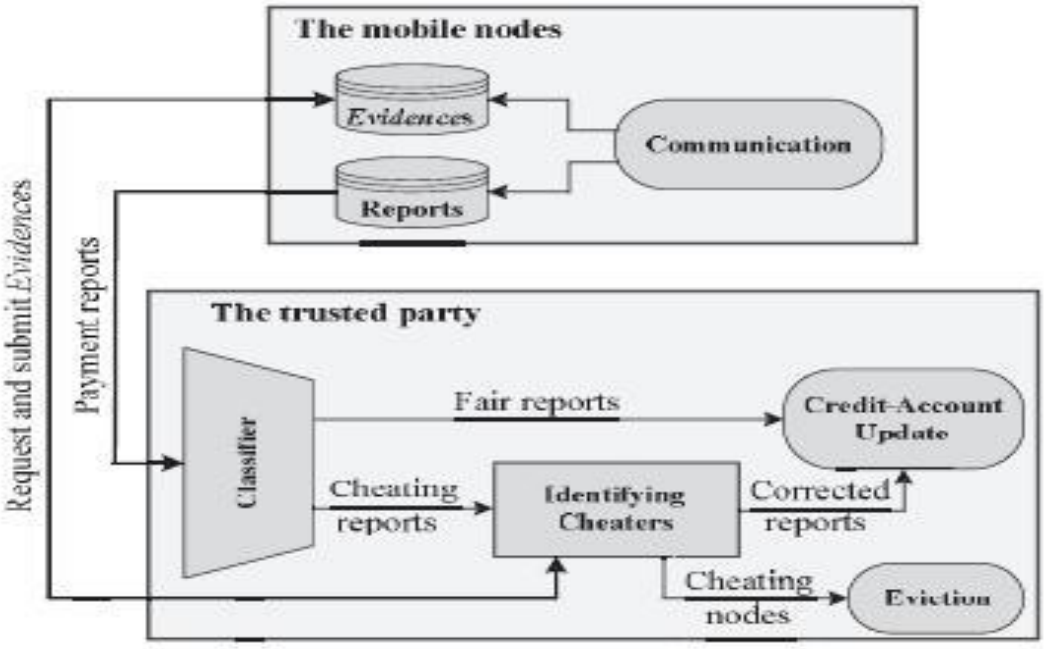

Fig 1.1 Architecture of RACE

The Communication phase has four processes: route establishment, data transmission, Evidence composition, and payment report composition/submission. Route establishment. In order to establish an end-to-end route, the source node broadcasts the Route Request (RREQ) packet containing the identities of the source (IDS) and the destination (IDD) nodes, time stamp (Ts), and Time-To-Live (TTL). TTL is the maximum number of intermediate nodes. After a node receives the RREQ packet, it appends its identity and broadcasts the packet if the number of intermediate nodes is fewer than TTL. The destination node composes the Route Reply (RREP) packet for the nodes broadcasted the first received RREQ packet, and sends the packet back to the source node.

A. Algorithm of Data transmission of Evidence and report

Algorithm 1: Data transmission/composition of *Evidence* and report

```
1: // ni is the source, intermediate, or destination node that is running
the algorithm.
2: if (ni is the source node) then
3:       PX ←[R, X, Ts, MX, SigS(R, X, Ts, H(MX ))];
4:       Send(PX);                  // send PX to the first node in the route
5: else
6:       if ((R, X, Ts are correct) and Verify(SigS(R, X, Ts, H(MX))) ==
                                                              TRUE) then
7:                if (ni is an intermediate node) then
8:                   Relay the packet;
9:                   Store SigS(R, X, Ts, H(MX));
10:               end if
11:               if (ni is the destination node) then
12:                  Send(h(X));
13:               end if
14:      else
15:               Drop the packet;
16:               Send error packet to the source node;
17:      end if
18: end if
19:  if (PX is last packet) then
20:      Evidence = {R, X, Ts, H(MX), h(0), h(X),H(SigS(R, X, Ts,
                                        H(MX)), SigD(R, Ts, h(0)))};
21:      Report = {R, Ts, F, X};
22:      Store Report and Evidence;
23:  end if
```

Data transmission. The source node sends data packets to the destination node through the established route and the destination node replies with ACK packets. For the Xth data packet, the source node appends the message MX and its signature to R, X, Ts, and the hash value of the message and sends the packet to the first node in the route. The security tokens of the Xth data and ACK packets are illustrated in Fig.3. The source node's signature is an undeniable proof for transmitting X messages and ensures the message's authenticity and integrity. Signing the hash of the message instead of the message can reduce the Evidence size because the smaller-size is attached to the Evidence instead of MX. Before relaying the packet, each intermediate node verifies the signature to ensure the message's authenticity and integrity, and verifies R and X to secure the payment. Each node stores only the last signature for composing the Evidence, which is enough. The data transmission process ends when the source node transmits its last message, or if the route is broken, e.g., due to node mobility or channel impairment. Algorithm 1 gives the pseudo code of the processes of data transmission and composition of Evidence and report.

IV. PROBLEM DESCRIPTION

The existing credit card payment schemes are designed for different system and threat models, which are infeasible for

MWNs. Selfish nodes will not relay others' packets and make use of the cooperative nodes to relay their packets, which degrades the network connectivity and fairness. The fairness issue arises when the selfish nodes make use of the cooperative nodes to relay their packets without any contribution to them, and thus the cooperative nodes are unfairly overloaded because the network traffic is concentrated through them. The selfish behavior also degrades the network connectivity significantly, which may cause the multihop communication to fail.

1. The existing receipt-based payment schemes impose significant processing and communication overhead and implementation complexity
2. Trusted party may not be involved in communication sessions, the nodes compose proofs of relaying others' packets, called receipts, and submit them to an offline accounting center (AC) to clear the payment
3. The AC has to apply a large number of cryptographic operations to verify the receipts, which may require impractical computational power and make the practical implementation of these schemes complex or inefficient.

The RACE, a Report-based pAyment sChemE for MWNs. The nodes submit lightweight payment reports (instead of receipts) to the AC to update their credit accounts, and temporarily store undeniable security tokens called evidences. The reports contain the alleged charges and rewards of different sessions without security proofs, e.g., signatures. The AC verifies the payment by investigating the consistency of the reports, and clears the payment of the fair reports with almost no cryptographic operations or computational overhead.

For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports, e.g., to steal credits or pay less. In other words, the Evidences are used to resolve disputes when the nodes disagree about the payment. Instead of requesting the Evidences from all the nodes participating in the cheating reports, RACE can identify the cheating nodes with submitting and processing few Evidences. Moreover, Evidence aggregation technique is used to reduce the storage area of the evidences.

V. CONCLUSIONS

The protocol RACE, a report-based payment scheme for MWNs. The nodes submit lightweight payment reports containing the alleged charges and rewards (without proofs), and temporarily store undeniable security tokens called Evidences. The fair reports can be cleared with almost no cryptographic operations or processing overhead, and Evidences are submitted and processed only in case of cheating reports in order to identify the cheating nodes. The analytical and simulation results demonstrate that RACE can significantly reduce the communication and processing overhead comparing to the existing receipt-based payment schemes with acceptable payment clearance delay and

Evidences' storage area, which is necessary for the effective implementation of the scheme. Moreover, RACE can secure the payment, and identify the cheating nodes precisely and rapidly without false accusations or missed detections.

In RACE, the AC can process the payment reports to know the number of relayed/dropped messages by each node. A trust system based on processing the payment reports to maintain a trust value for each node is developed. Based on these trust values, a trust-based routing protocol to route messages through the highly trusted nodes to minimize the probability of dropping the messages, and thus improve the network performance in terms of throughput and packet delivery ratio. However, the trust system should be secure against singular and collusive attacks, and the routing protocol should make smart decisions regarding node selection with low overhead.

ACKNOWLEDGMENT

This work was supported by R.V.S Faculty of Engineering in Computer Science Engineering Department of Coimbatore.

REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications Over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[3] H. Gharavi, "Multichannel Mobile Ad Hoc Links for Multimedia Communications," Proc. IEEE, vol. 96, no. 1, pp. 77-96, Jan. 2008.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom '00, pp. 255-265, Aug. 2000.

[5] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation Enforcement Schemes for MANETs: A Survey," Wiley's J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332, 2006.

[6] Y. Zhang and Y. Fang, "A Secure Authentication and Billing Architecture for Wireless Mesh Networks," ACM Wireless Networks, vol. 13, no. 5, pp. 663-678, Oct. 2007.

[7] L. Buttyan and J. Hubaux, "Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 8, no. 5, pp. 579-592, Oct. 2004.

[8] Y. Zhang, W. Lou, and Y. Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks," ACM Wireless Networks, vol. 13, no. 5, pp. 569-582, Oct. 2007

