ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 2, February 2016

# Defending against Collaborative Attack's in MANET

**Nilesh Patil [1], Sagar Patil [2], Ravindra Raut [3], Vaibhav Thorat [4]**

UG Student, Dept. Of Computer Engineering.,SKN Sinhgad Institute of science & Tech., Lonavala, (MS), India[1, 2, 3, 4]

***ABSTRACT***— In mobile ad hoc networks (MANETs), an essential requirement for the foundation of communication among nodes is that nodes should coordinate with one another. In the presence of malicious nodes, this requirement may lead serious security concerns; for instance, such node may disturb the routing process. In this context, preventing or detecting malicious nodes launching gray hole or collaborative black hole in challenge. This project attempts to determine this issue by designing a dynamic source routing (DSR)- based routing mechanism, which is referred to as the cooperative bait detection scheme(CBDS), that coordinates the advantages of both proactive and reactive defense architectures. Our CBDS system implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics).

***KEYWORDS*** – Cooperative bait detection scheme (CBDS), collaborative bait detection, collaborative blackhole attacks, detection mechanism, dynamic source routing (DSR), gray hole attacks, Malicious node, mobile ad hoc network (MANET).

## I. INTRODUCTION

Due to the widespread availability of mobile devices, mobile ad hoc networks (MANETs), have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property. In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 2, February 2016

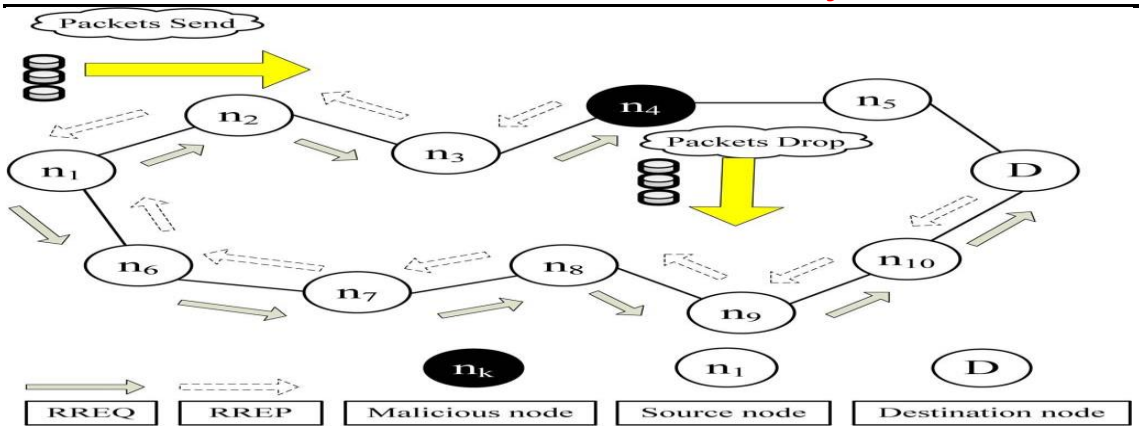



**Fig. 1.Blackhole attack–node n4 drops all the data packets.**

This is primarily due to their infrastructure less property. In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network [3]. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations.

Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. Ithis regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as black hole and gray hole (known as variants of black hole attacks). In black hole attacks (see Fig. 1), a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a malicious node (so-called black hole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that “fake” shortest route to the destination and then discard these packets without forwarding them to the destination. In gray hole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. In this paper, our focus is on detecting grayhole/collaborative blackhole attacks using a dynamic source routing (DSR)-based routing technique.

## II. LITURATURE SURVEY

Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves are responsible for the creation, operation and maintenance of the network . The topology of the network varies rapidly and unpredictably over time due to mobility of the nodes. Topology varies in the way that a group of nodes may connect together to form a large network and later they may split to form smaller groups. Performance of MANET depends upon routing protocols, battery consumption, bandwidth etc. Routing is done using various routing protocols. The open medium, dynamic characteristics and lack of central infrastructure characteristics

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 2, February 2016

make MANETs susceptible to various security threats that degrade the performance of the network in terms of reliability and throughput[5].Watchdog is used intensively in many solutions for the cooperation problem. The main drawback of this idea is that it enables selfishness and misbehaving nodes to transmit packets without punishing them, and thus encourages misbehavior. We propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid multiple black holes acting in the group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. Our solution assumes that nodes are already authenticated and hence participate in communication. Assuming this condition, the black hole attack is discussed Our approach to combat the Black hole attack [2].

In this approach, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list [3].

**EXISTING SYSTEM:**

DSR involves two main processes: route discovery and route maintenance. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. If an intermediate node has routing information to the destination in its route cache, it will reply with a RREP to the source node. When the RREQ is forwarded to a node, the node adds its address information into the route record in the RREQ packet. When destination receives the RREQ, it can know each intermediary node's address among the route. The destination node relies on the collected routing information among the packets in order to send a reply RREP message to the source node along with the whole routing information of the established route.

**DISADVANTAGES OF EXISTING SYSTEM:**

- The lack of any infrastructure added with the dynamic topology feature of MANETs makes these networks highly vulnerableble to routing attacks such as black hole and grayhole (known as variants of blackhole attacks).
- In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network

## III. PROPOSED SOLUTION

In this paper, a mechanism called "cooperative bait detection scheme" (CBDS) is presented that effectively detects the malicious nodes that attempt to launch grayhole/collaborative blackhole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

**ADVANTAGES OF PROPOSED SYSTEM:**

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 2, February 2016

• 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.

This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes.

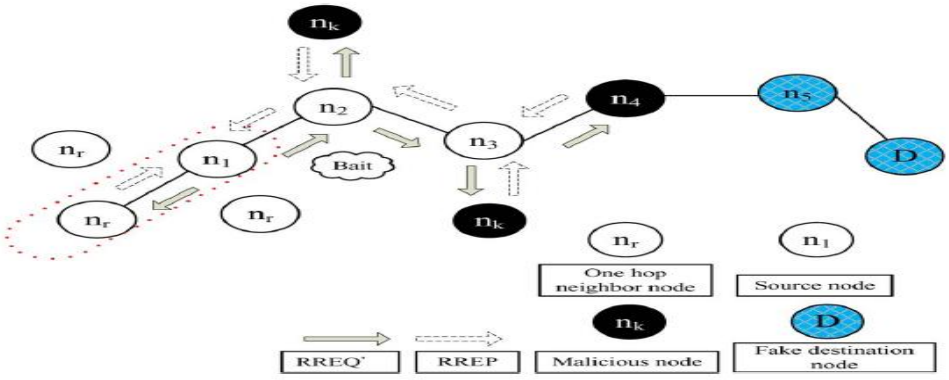



**Fig. 2. Operations of the CBDS.**

| Option Type | Opt Data Len | Request ID |
|---|---|---|
| Target Address (RREQ' : Bait address) | | |
| Address[1] | | |
| Address[2] | | |
| ..... | | |
| Address[n] | | |

The CBDS scheme comprises three steps: 1) the initial bait step; 2) the initial reverse tracing step; and 3) the shifted to reactive defense step, i.e., the DSR route discovery start process. The first two steps are initial proactive defense steps, whereas the third step is a reactive defense step.

**A. Initial Bait Step**

The goal of the bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted. To achieve this goal, the following method is designed to generate the destination address of the bait RREQ.

The source node stochastically selects an adjacent node, i.e., nr, within its one-hop neighbourhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ. Since each baiting is done stochastically and the adjacent node would be changed if the node moved, the bait would not remain unchanged. This is illustrated in Fig. 2, The bait phase is activated whenever the bait RREQ is sent prior to seeking the initial routing path. The follow-up bait phase analysis procedures are as follows.

First, if the nr node had not launched a blackhole attack, then after the source node had sent out the RREQ, there would be other nodes' reply RREP in addition to that of the nr node. This indicates that the malicious node existed in the reply routing, as shown in Fig. 2. Therefore, the reverse tracing program in the next step would be initiated in order to detect this route. If only the nr node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDS had initiated the DSR route discovery phase.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 2, February 2016

Second, if nr was the malicious node of the blackhole attack, then after the source node had sent the RREQ, other nodes (in addition to the nr node) would have also sent reply RREPs. This would indicate that malicious nodes existed in the reply route. In this case, the reverse tracing program in the next step would be initiated to detect this route. If nr deliberately gave no reply RREP, it would be directly listed on the blackhole list by the source node. If only the nr node had sent a reply RREP, it would mean that there was no other malicious node in the network, except the route that nr had provided; in this case, the route discovery phase of DSR will be started. The route that nr provides will not be listed in the choices provided to the route discovery phase.

**B. Initial Reverse Tracing Step**

The reverse tracing program is used to detect the behaviours of malicious nodes through the route reply to the RREQ message. If a malicious node has received the RREQ, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route. It should be emphasized that the CBDS is able to detect more than one malicious node simultaneously when these nodes send reply RREPs. Indeed, when a malicious node, for example, nm, replies with a false RREP, an address list P = {n1,...nk,...nm,...nr} is recorded in the RREP. If node nk receives the RREP, it will separate the P list by the destination address n1 of the RREP in the IP field and get the address list Kk = {n1,...nk}, where Kk represents the route information from source node n1 to destination node nk. Then, node nk will determine the differences between the address list P = {n1,...nk,...nm,...nr} recorded in the RREP and Kk = {n1,...nk}. Consequently, we get (1)mwhere represents the route information to the destination node (recorded after node nk). The operation result of is stored in the RREP's "Reserved field" and then reverted to the source node, which would receive the RREP and the address list of the nodes that received the RREP. To avoid interference by malicious nodes and to ensure that does not come from malicious nodes, if node nk received the RREP, it will compare:

**ALGORITHM:**

**Dynamic Threshold Algorithm**

```
01  double threshold=0.9;
02  InitialProactiveDefense( );
03  double Dynamic(threshold)
04  {  double T1, T2;
05        T1=calculate the time of PDR down to threshold;
06        if(PDR < threshold)
07        InitialProactiveDefense( );
08        T2=calculate the time of PDR down to threshold;
09        if(T2 < T1){
10          if(threshold < 0.95)
11          threshold=threshold+0.01;
12        }
13        else{
14            if(threshold > 0.85)
15            threshold=threshold-0.01;
16        }
17        if(SimulationTime < 800){
18        return threshold;
19        Dynamic(threshold);
20        }
21        else
22        return 0.9;
23  }
24
```

.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 2, February 2016

## IV. PERFORMANCE EVALUATION

### A. Simulation Parameters

The QualNet 4.5 simulation tool [16] is used to study the performance of our CBDS scheme. We employ the IEEE 802.11 [17] MAC with a channel data rate of 11 Mb/s. In our simulation, the CBDS default threshold is set to 90%. All remaining simulation parameters are captured in Table III. The network used for our simulations is depicted in Fig. 5; and we randomly select the malicious nodes to perform attacks in the network.

### B. Performance Metrics

We have compared the CBDS against the DSR [4], 2ACK [9], and BFTR [13] schemes, chosen as benchmarks, on the basis of the following performance metrics.

Packet Delivery Ratio: This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, pktdi is the number of packets received by the destination node in the ith application, and pktsi is the number of packets sent by the source node in the ith application. The average packet delivery ratio of the application traffic n, which is denoted by PDR, is obtained as . (4)

Routing Overhead: This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. Here, cpki is the number of control packets transmitted in the ith application traffic, and pkti is the number of data packets transmitted in the ith application traffic. The average routing overhead of the application traffic n, which is denoted by RO, is obtained as . (5)

Average End-to-End Delay: This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is di, and the number of packets received by the destination node is pktdi. The average end-to-end delay of the application traffic n, which is denoted by E, is obtained as . (6)

Throughput: This is defined as the total amount of data (bi) that the destination receives them from the source divided by the time (ti) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic n, which is denoted by T, is obtained as . (7)

## TABLE III

SIMULATION PARAMETERS

| Parameter | Value |
|---|---|
| *Application traffic* | *10 CBR* |
| *Transmission rate* | *4 packets/s* |
| *Radio range* | *250m* |
| *Packet size* | *512 bytes* |
| *Channel data rate* | *11Mbps* |
| *Pause time* | *0s* |
| *Maximum Speed* | *20m/s* |
| *Simulation time* | *800s* |
| *Number of nodes* | *50* |
| *Area* | *700m*700m* |
| *Malicious nodes* | *0% 40%* |
| *Threshold* | *Dynamic threshold* |

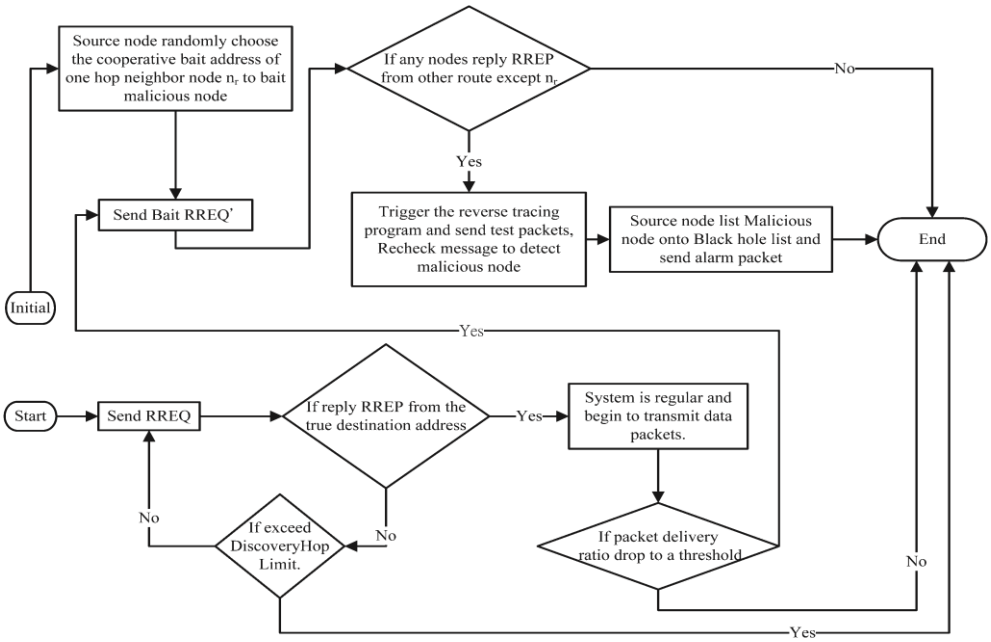
Two simulation scenarios are considered:

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 2, February 2016

1) Scenario 1: Varying the percentage of malicious nodes with a fixed mobility.

2) Scenario 2: Varying the mobility of nodes under fixed percentage of malicious nodes.

Under these scenarios, we study the effect of different thresholds of the CBDS on the aforementioned performance parameters. The results are as follows.




**C. Varying the Percentage of Malicious Nodes With a Fixed Mobility**

First, we study the packet delivery ratio of the CBDS and DSR for different thresholds when the percentage of malicious nodes in the network varies from 0% to 40%. The maximum speed of nodes is set to 20 m/s. Here, the threshold value is set to 85%, 95%, and the dynamic threshold, respectively. The results are captured in Fig. 6. In Fig. 6, it can be observed that DSR drastically suffers from blackhole attacks when the percentage of malicious nodes increases. This is attributed to the fact that DSR has no secure method for detecting/preventing blackhole attacks. Our CBDS scheme shows a higher packet delivery ratio compared with that of DSR. Even in the case where 40% of the total nodes in the network are malicious, the CBDS scheme still successfully detects those malicious nodes while keeping the packet delivery ratio above 90%. A threshold of 95% would then result in earlier route detection than when the threshold is 85% or is set to the dynamic threshold value. Thus, the packet delivery ratio when using a threshold of 95% is higher than that obtained when using a threshold of 85% or the dynamic threshold.

Second, we study the routing overhead of the CBDS and DSR for different thresholds. The results are captured in Fig. 7. In Fig. 7, it can be observed that when the number of malicious nodes increases, DSR produces the lowest routing overhead compared with the CBDS. This is attributed to the fact that DSR has no intrinsic security method or defensive mechanism. In fact, the routing overhead produced by the CBDS for different thresholds is a little bit higher than that produced by DSR; this might be due to the fact that the CBDS would first send bait packets in its initial bait phase and then turn into a reactive defensive phase afterward. Consequently, a tradeoff should be made between routing overhead and packet delivery ratio. We have studied the effect of thresholds on the routing overhead. As expected, it was found that the routing overhead of the CBDS reaches the highest value when the threshold is set to

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 2, February 2016

## V. CONCLUSION

In this paper, we developed a ranking fraud detection system for mobile Apps. Specifically, we first showed that ranking fraud happened in leading sessions and provided a method for mining leading sessions for each App from its historical ranking records. Then, we identified ranking based evidences, rating based evidences and review based evidences for detecting ranking fraud. Moreover, we proposed an mining Leading session algorithm for obtain mining leading session and aggregation method. In the future, we plan to study more effective fraud evidences and analyse the latent relationship among rating, review and rankings. Moreover, we will extend our ranking fraud detection approach with other mobile App related services, such as mobile Apps recommendation, for enhancing user experience.

## REFERENCES

[1] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," J. Mach. Learn. Res., pp. 993–1022, 2003.

[2] Y. Ge, H. Xiong, C. Liu, and Z.-H. Zhou, "A taxi driving fraud detection system," in Proc. IEEE 11th Int. Conf. Data Mining, 2011, pp. 181–190.

[3] D. F. Gleich and L.-h. Lim, "Rank aggregation via nuclear norm minimization," in Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2011, pp. 60–68.

[4] A. Klementiev, D. Roth, K. Small, and I. Titov, "Unsupervised rank aggregation with domain-specific expertise," in Proc. 21st Int. Joint Conf. Artif. Intell., 2009, pp. 1101–1106.

[5] A. Klementiev, D. Roth, and K. Small, "Unsupervised rank aggregation with distance-based models," in Proc. 25th Int. Conf. Mach. Learn., 2008, pp. 472–479

[6] Hengshu Zhu, Hui Xiong, Senior Member, IEEE, Yong Ge, and Enhong Chen, Senior Member, IEEE, "Discovery of Ranking Fraud for Mobile Apps", vol.13,n0.1,Jan 2015

[7] A. Ntoulas, M. Najork, M. Manasse, and D. Fetterly, "Detecting spam web pages through content analysis," in Proc. 15th Int. Conf. World Wide Web, 2006, pp. 83–92.

[8] N. Spirin and J. Han, "Survey on web spam detection: Principles and algorithms," SIGKDD Explor. Newslett., vol. 13, no. 2, pp. 50– 64, May 2012.

[9] B. Zhou, J. Pei, and Z. Tang, "A spamicity approach to web spam detection," in Proc. SIAM Int. Conf. Data Mining, 2008, pp. 277–288.

[10] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in Proc. 19thACMInt. Conf. Inform. Knowl. Manage., 2010, pp. 939–948

[11] Z. Wu, J. Wu, J. Cao, and D. Tao, "HySAD: A semi-supervised hybrid shilling attack detector for trustworthy product recommendation," in Proc. 18th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2012, pp. 985–993.

[12] S. Xie, G. Wang, S. Lin, and P. S. Yu, "Review spam detection via temporal pattern discovery," in Proc.