iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** XI **Month of publication:** November 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Selfish Nodes Detection Techniques in MANET-A Survey

Aniket Patil[1],Javed Khan[2],Ashish Khandave[3],Abhishek Yadgire[4],Prof. Monika Dangore[5]
[1,2,3,4,5] *Department of Computer Engineering, Dr. D.Y. Patil School Of Engineering, Lohegaon, Pune-411015*

Abstract: ***Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. A mobile ad hoc network (MANET) is an infrastructure-less network of mobile devices connected without wires, sometimes untrustworthy. From last decade, mobile ad hoc networks have become a very popular research topic. Communication range among mobile nodes in ad-hoc network is limited; hence several hops are needed in a network to transmit a packet from one node to another node. In mobile ad hoc network, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes as it is a cost intensive activity. This behaviour of selfish nodes could then degrade the overall data accessibility which results into performance degradation of overall network. We surveyed some key technique for detecting selfish nodes in MANET.This paper provides a survey on different technique used to detect selfish nodes in such network as well as compare them (to study)in order to reduce the effect of selfish nodes in mobile ad hoc networks. Moreover one important aspects of this paper is to propose specific technique that would evaluate the selfishness behaviour of nodes in the network in less time and effectively.***
Keyword: Mobile Ad hoc Networks (MANET) ,Self-configuring, Infrastructure-less ,Cost-intensive, Selfish nodes.

I. INTRODUCTION

In Wireless mobile ad hoc networks nodes are free to move as well as network is self-configuring and dynamic. A mobile ad hoc network (MANET) is a network of mobile devices connected without wires which does not require any infrastructure.. Ad hoc means "for this purpose" in LATIN. Each device in a MANET can freely move in any direction independently and can link itself to any other device frequently. Setting up of fixed access points and backbone infrastructure is not possible in a disaster area or war zone. Infrastructure for short-range radios; Bluetooth (range ~ 10m) may not be practical.

Ad hoc networking is a combination of network elements that forms a network requiring little or no planning. The network is ad hoc because it does not require any pre-existing infrastructure, such as routers in wired networks or access points in managed wireless networks. Rather, each node takes part in transmitting data to other nodes, so dynamically on the basis of network connectivity those nodes which forwards data are determined. Dynamic Source Routing [DSR] and AODV are some algorithms that have been designed to handle such transmission of data [2].

Applications of mobile ad hoc networks have been developed mainly for crisis situations (e.g. natural disasters, military conflicts and emergency medical situations). In these applications, all the nodes of the network have a common goal and belong to a single authority. With the progress of technology, it has now become possible to deploy mobile ad hoc networks for real time applications as well. Some applications are networks of cars parking and provision of communication facilities in remote areas. In such networks nodes do not belong to a single authority and they do not pursue a common goal. In addition, these networks could be huge long-lasting, and self-organizing as well. In such networks, there is no good reason to assume that the nodes cooperate. Indeed, It is true: In order to save resources (e.g., battery power, memory, CPU cycles) the nodes tend to be “selfish”.

On the basis of survey done so far, there are two main strategies which help to deal with selfish behaviour: a) motivation or incentive based approaches, and b) detection and exclusion. The first approach, tries to motivate nodes to actively participate in the forwarding activities [16].The detection and exclusion approach is a straight-forward way to cope with selfish nodes and several solutions have been presented [1], [3], [4].

Impact of node selfishness on MANETs has been studied in [5]. In [7] it is shown that when no selfishness prevention mechanism is present, the packet delivery rates are reduced by high margin, from a rate of 80% when the selfish node ratio is 0, to 30% when the selfish node ratio is 50%. The survey [6] shows similar results: the number of packet losses is increased by 500% when ratio of selfish node rises from 0% to 40%. A more detailed study [5] shows that a moderate concentration of node selfishness (starting from a 20% level) has a huge impact on the overall performance of MANETs, like the offered throughput, probability of reach-ability,

©IJRASET 2015: All Rights are Reserved

average hop count and the number of packets dropped. In DTNs, the performance of packet transmission can be seriously degraded by selfish behaviour of nodes. For example, in two-hop relay schemes, selfish node does not retransmit the packet received, therefore being lost. Therefore, for the overall performance of the network, detecting such nodes quickly and accurately is essential.
This paper provides a survey on different technique used to detect selfish nodes in such network as well as compare them in order to reduce the effect of selfish nodes in mobile ad hoc networks. The paper comprises of following section: Related work: shows the literature study, Methods to detect selfish nodes: explains various methods used to detect selfish nodes in a network, Conclusion and Future Work.

II. RELATED WORK

Literature studied shows that there are various technique to detect selfish node, some of them are studied and explained below. Techniques used to detect selfish nodes can be classified into three categories:

A. A Reputation-Based Technique

Reputation based technique depends on building a reputation metric for each node according to its behavioral pattern. A Watchdog is used by most of the systems as monitoring method. Watchdog was proposed by Marti et al. [10] to detect data packet non forwarding by overhearing the transmission of the next node. [13], [14], [15] not only use same monitoring technique but also transmits the collected information to nearby nodes. Basically, Reputation is the amount of trust achieved by a member of a community in a specific domain of interest. There are three types of Reputation schemes:

Subjective Reputation.

Indirect Reputation.

Functional Reputation

B. Credit Based Technique

In credit based technique incentives are provided on the basis how the networking functions are performed by a node. To achieve this goal, virtual (electronic) currency or some kind of monetary system may be set up. Nodes are rewarded with incentives for providing services to other nodes. Even those nodes are paid who are requested for their services by the same payment system. There are two models used for implementation of Credit based schemes:

The Packet Trade Model (PTM) [2] and

The Packet Purse Model (PPM).

C. Acknowledgement Based Technique

The ACK based techniques rely on the reception of an acknowledgment to verify that a packet has been forwarded. Liu et al. [11] proposed the 2ACK system where acknowledgment is send to two upstream hops explicitly by nodes in order to verify their co-operation. This system is susceptible to collusion of two or more consecutive nodes. colluding nodes can claim to not receive the acknowledgement by framing the honest nodes.
All mechanisms mentioned above were put forward for detection and handling of misleading nodes.

III. METHODS TO DETECT SELFISH NODES

Some methods to detect selfish nodes in MANET are discussed below

A. Watchdog

In Kachirski O et. al. [19], misbehaving nodes are identified on the basis of packet dropped during the transmission of the next hop. When a node forwards packets, proper transmission of packets by the next node is verified by Watchdog. Misbehavior is noticed, If that node refuses to transmit the packets. The misbehaving nodes can be identified in the level of connection as well as in forwarding level, which is an advantage of Watchdog. It means it identifies nodes in the link layer as well as in the network layer. Watchdog is easy to implement. In Kachirski O et. al. [19], Watchdog has some drawbacks, Identifying misbehaving nodes may be difficult because of lack of cooperation in nodes under circumstances such as 1) false misbehaving 2) minor dropping. 3) limited

©IJRASET 2015: All Rights are Reserved

transmission power 4) ambiguous collision 5) collision 6) receiver collision

B. Pathrater

In Kachirski O et. al. [19], "Path metric" is calculated for every path by this technique. Each node has a pathrater same as that of nodes in watchdog technique has. The node maintains a degree of other nodes identified in the network. From past experience, the path metric is calculated by the combination of node rating with link reliability. The Pathrater chooses the path with highest metric after calculation of path metric for all reachable paths.

C. Collaborative Watchdog Method

The Watchdog mechanism overhear wireless traffic and analyses it to decide whether neighbor nodes are behaving in a selfish manner and also detects the selfish nodes in the networks. The nodes other than the selfish nodes in the network can be called as collaborative nodes. Collaborative watchdog indicates the presence of the selfish node to the source node. The source node then broadcasts the selfish information to all other nodes. When a selfish node is detected it is marked as positive,(or negative if not) or no info when dissatisfying both the above. This approach reduces the detection time and improves the precision by reducing the effect of both false positives and false negatives.

D. Confidant

[23]. Confidant stands for Cooperation of Nodes Fairness in Dynamic Ad-hoc Network .Its aim is to detect and isolate selfish nodes thus making it unattractive to deny cooperation. It is a reputation based system in which routing and forwarding is evaluated according to network protocol and the nodes monitor their neighbors and change their reputation accordingly. Participation in the Confidant meta-protocol is evaluated using trust. Trust is established on the basis of experience, observation or reported routing and forwarding behavior of other nodes. Main components of Confidant are The Monitor, The Trust Manager, The Reputation System and the Path Manager. In Monitoring the nodes keep a watch on the neighbor nodes by either listening to their transmission or by observing their routing behavior. The trust manager handles the incoming and outgoing ALARM messages and sends ALARM messages to other nodes to make them aware about the malicious nodes. The nodes themselves create outgoing messages when they experience, observe or receive a report of some malicious behavior. The reputation system consists of a table which has entries for nodes and their rating and a node is only considered as malicious if there sufficient evidence about its malicious behavior. The functions of Path manager includes path re-ranking according to reputation of the nodes in the path, action on receiving a request for a route from a malicious node, deletion of paths containing malicious nodes.

In spite of detecting and isolating misbehaving nodes it has some limitations:-

It is a detection-based reputation system.

Events have to be observable and classified for detection.

Reputation can only be meaningful if the identity of each node is persistent; otherwise it is vulnerable to spoofing attack.

E. Incentive-Based Detection

[22]. In this, informant approach that is based on economical incentive policy which is a general solution that does not belong to a specific application domain. An entity named Detective rewards sibyls identities if they reveal themselves. The name of the target peer and a security deposit is given to the detective by an identity while the target peer receives the deposit and a certain reward. The minimum reward for revealing a Sybil node is decided by a Dutch auction. Informant has some positive characteristics. An attacker is revealed when the attackers aversion of being detected is less than the detective's interest of detecting it[24]. Detective gets benefitted when the presence of highly averse Sybil attacker does not deter it from participating in the underlying peer-to-peer application. Informant relies on some form of anonymous payment but due to lack of practical electronic cash it becomes an obstacle for implementation.

F. Recurring Cost And Fees

Each node participating in the network is charged with a fee. It is either charged periodically or just one time. Identities i.e. the nodes are re-validated after a period. It was concluded by Margolin that recurring fee is a stronger deterrent as compared to onetime fee. The recurring is not money based mechanism rather it is can be CAPTCHAS , charged SMS or cooperation in network which is a non-monetary mechanism. But this technique may be inadequate in preventing the attack as a Sybil node may incur only a one-time cost which can be easily recovered by executing an attack. An attack is successfully only if the attackers objective value

©IJRASET 2015: All Rights are Reserved

exceeds the threshold value. Hence using recurring fees Sybil attacks can be reduced to some extent.

G. 2ACK Method

The acknowledgement-based 2ACK scheme is used to reduce the adverse effects of misbehaving nodes. The basic idea of TWOACK method is to, when a data packet is forwarded by a node successfully over the next hop, the next-hop-link's destination node will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. The 2ACK method is used to detect misbehaving links and to reduce their effects. For an existing protocol of MANET like DSR, 2ACK method can be introduced as an add-on. The misbehavior is detected through a new type of acknowledgement packet called as 2ACK. A fixed route of two hops is assigned to the 2ACK packet which is in the opposite direction of the data traffic route [18]. At destination, a hash code will be generated and compared with the sender's hash code to check the confidentiality of message. Hence, if the link is misbehaving, sender to transmit messages will not use it in future and loss of packets can be avoided.

H. S-2ACK Method

A derivative of the basic 2ACK scheme called as S-2ACK scheme aims at minimizing the overhead of routing and not only guarantees the improvement in performance but also handles the false alarms problem caused by 2ACK packets lost. The difference between S-2ACK and 2ACK is that 2ACK packet in 2ACK acknowledges one data packet whereas in S-2ACK scheme even the receipt of number of packets is acknowledged. But when both are compared the 2ACK scheme handles the trade-off in a better way between the performance of network and the cost. [18].

IV. CONCLUSION

As we know how the selfish or malicious nodes in ad hoc networks are detected, but it's a complex task. This survey paper considers number of different techniques that can detect selfish nodes .From this survey, we conclude that the reputation based scheme i.e. Collaborative Watchdog is the most efficient technique for detecting selfish nodes. Analytical and experimental results show that it can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost).

V. FUTURE WORK

One problem that remains with our current simulations is that in order to get good detection results , all the thresholds need to be set manually. So in the future we will try to find ways how these values can be set and adjusted automatically during operation. We plan to study how we can provide more effective infrastructure-free authentication in ad hoc networks assuming that identities need not be entirely stable at the routing level, but that spoofing of other nodes is unacceptable.

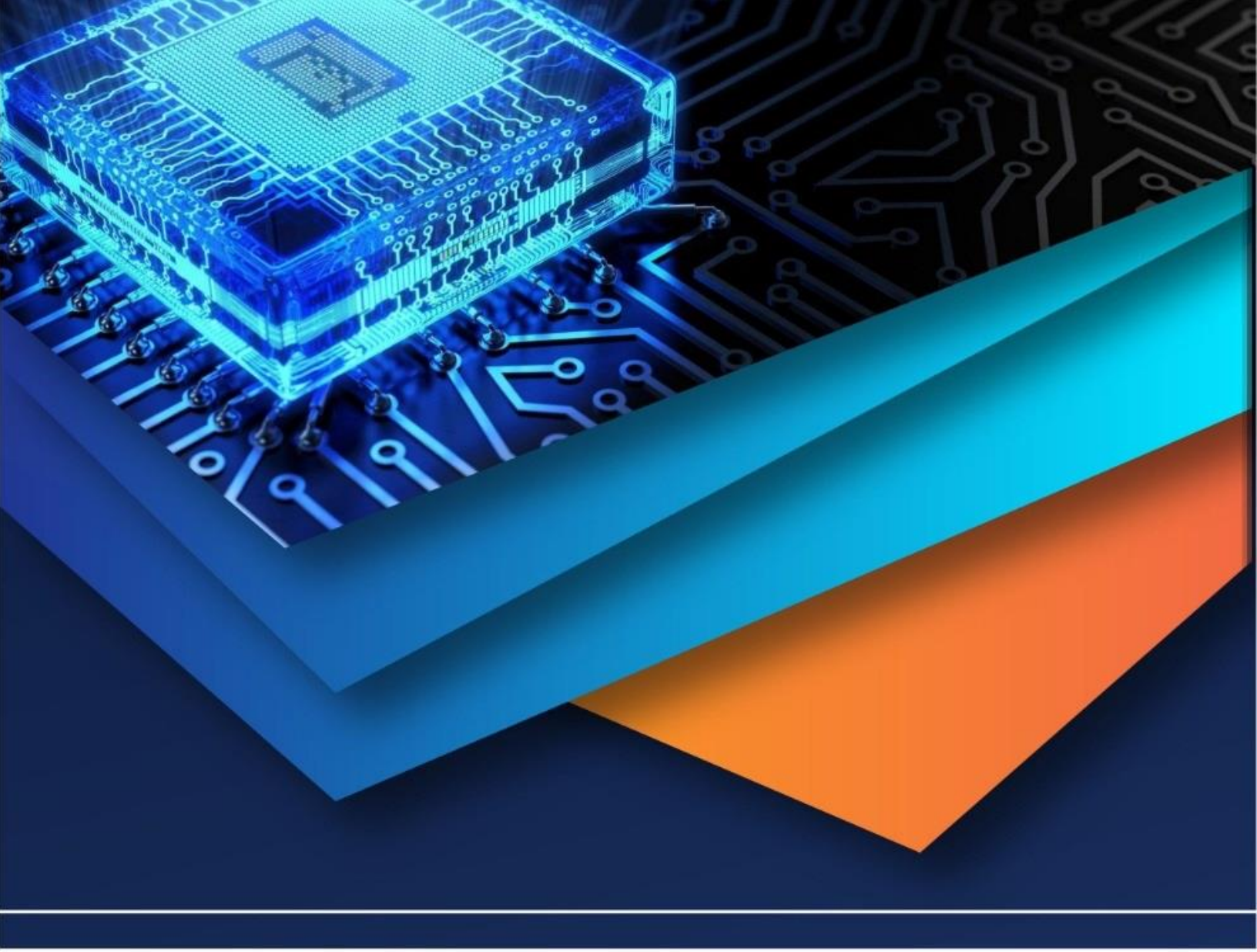
REFERENCES

[1] 1] S. Buchegger and J.-Y. Le Boudee. Self-policing mobile ad hoc networks by reputation systems. Communications Magazine, IEEE, 43(7):101 – 107, jul. 2005.
[2] KhairulAzmi Abu Bakar and James Irvine "Contribution Time-based Selfish Nodes Detection Scheme" ISBN: 978-1-902560-24-3 © 2010 PGNet
[3] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz. On the effect of node misbehavior in ad hoc networks. In Proceedings of IEEE International Conference on Communications, ICC'04, pages 3759–3763. IEEE, 2004.
[4] M. Karaliopoulos. Assessing the vulnerability of DTN data relaying schemes to node selfishness. Communications Letters, IEEE, 13(12):923–925, december 2009.
[5] C. K. N. Shailender Gupta and C.Singla. Impact of selfish node concentration in MANETs. International Journal of Wireless and MobileNetworks (IJWMN), 3(2):29–37, Apr 2011.
[6] C. Toh, D. Kim, S. Oh, and H. Yoo. The controversy of selfish nodes in ad hoc networks. In Proceedings of Advanced CommunicationTechnology (ICACT), volume 2, pages 1087 –1092, feb. 2010.
[7] Y. Yoo, S. Ahn, and D. Agrawal. A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks. In Proceedings of IEEEICC, volume 5, pages 3005 – 3009 Vol. 5, may 2005.
[8] J. R. Douceur, "The Sybil attack," presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.
[9] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat "Lightweight Sybil Attack Detection in MANETs" 1932-8184/$31.00 _c 2012 IEEE
[10] S. Marti, T. Giuli, K. Lai, and M. Bakar, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom'00), August 2000, pp. 255–265.
[11] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," in IEEE Transactions on Mobile Computing, 2006, pp. 536–550.
[12] D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro, "On the use of radio resource tests in wireless ad hoc networks," in Proc. 3rd WRAITS, 2009, pp. 21–26.

©IJRASET 2015: All Rights are Reserved

[13] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputationbased incentive scheme for ad-hoc networks," in WCNC 2004, 2004.
[14] S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol: (cooperative of nodes – fairness in dynamic ad hoc networks)," in Proc. IEEE/ACM Workshop on (MobiHoc'02), June 2002, pp. 226–336.
[15] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in (CMS'02), September 2002.
[16] Butty´an, Levente, Hubaux, and Jean-Pierre. Enforcing service availability in mobile ad-hoc WANs. In Proceedings of MobiHoc'00, pages 87–96. IEEE Press, 2000.
[17] N. B. Margolin and B. N. Levine, "Quantifying resistance to the Sybil attack," in Financial Cryptography and Data Security. Berlin, Germany: Sprnger, 2008.
[18] K Balakrishnan, J Deng, and P K Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. And Networking, pp. 2137- 2142, 2005
[19] Kachirski O, Guha R. (2003). "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", in Proceeding IEEE, (HICSS'03), pp 57.1.
[20] Nasser N, Chen Y. (2007). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network, in Proceeding IEEE (ICC'07, pp 1154-9.
[21] J.Vijithanand et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012,5454-5461
a. www.ijcsit. A Survey on Finding Selfish Nodes in Mobile Ad Hoc Networks
[22] Int. J. Advanced Networking and Applications Volume: Issue: Pages: A Review of Techniques to Mitigate Sybil Attacks Nitish Balachandran Department of Computer Science and Information Systems, BITS Pilani
[23] Informant: Detecting Sybils Using Incen-tives N. Boris Margolin and Brian N. Levine Department of Computer Science, Univ. of Massachusetts, Amherst, MA, USA {margolin,brian}@cs.umass.edu.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)