AD HOC NETWORKS: FILTER BASED ADDRESSING PROTOCOL

Tanaya Mehendale[1], Y.D.Chincholkar[2]

[1]*Student, Electronics and Telecommunication, Sinhgad College of Engineering, Maharashtra, India*
[2]*Professor, Electronics and Telecommunication, Sinhgad College of Engineering, Maharashtra, India*

Abstract

Wireless networks are becoming more popular now-a-days. These networks can either be infrastructure based or infrastructure less networks. The infrastructure networks have a base station or central point of co-ordination. But in infrastructure less networks the base station or central point of contact is not present. They are termed as ad hoc networks. These networks dynamically change their topology and do not have any central point of contact. Main applications of such networks include rescue operations where laying down of wires is not possible, military applications or battle field operations. Addressing is a key issue in such type of networks. As they change their topology dynamically and also face frequent partition and merging events assigning addresses in such a network is a key issue. In this paper a dynamic addressing scheme which is dependent or filters is considered which assigns addresses to the nodes in the ad hoc network.

Keywords: *Ad hoc networks, AODV, Dynamic addressing protocol, Filter Signature, Hashing, and Sequence filter.*

----------***----------

1. INTRODUCTION

Whenever two or more devices want to exchange any kind of information they form a network. This network can be a LAN covering a building, or a MAN which covers a city or spread across the world which can be a WAN. All the networks formed for the purpose of communication either have an access point or a centre point of contact which manages the network or do not have any central point of contact. The former networks are called as infrastructure networks and later are the infrastructure less networks or ad hoc networks. The infrastructure network has fixed topology and central point of contact which is responsible for all the communication taking place between the devices or entities in the network. Exact opposite is the case with the ad hoc networks. The networks which are formed for purpose only are called as ad hoc networks. These networks are established for a particular purpose, this purpose can be exchange of information. Once the purpose is completed the connection is broken or terminated. They lack infrastructure and do not have any central point of co-ordination. Also the nodes in the network keep on changing the topologies with time. Any node or device taking part in communication is identified by a unique address. Addressing is a main and very important, challenge in ad-hoc networks as the nodes dynamically change their topology and lack central point of contact. Ad hoc networks cannot use any protocols like DHCP or Network Address Translation. A central server assigning the addresses to the devices is not possible in ad hoc networks which is used in DHCP.A unique addressing scheme based on sequence filters is proposed in this paper which not only dynamically assigns addresses to the nodes in the network but also with less amount of control overhead and more packet delivery ratio. Moreover to detect the partition and merging events a hashing is used instead of random numbers.

1.1 Need of Dynamic Addressing Scheme

Address collisions should be avoided. No two nodes at a given instant of time in the same partition should have same address. Security should also be considered. The protocol should check if the node joining a network is authorized node or an adversary node. If a node utilizing a particular IP address joins another partition its address should become available to other nodes in the networks. The protocol should consider the dynamically changing topology and partition and merging events in the network. Addresses should be assigned with less amount of control overhead and minimum delay [1].

2. LITERATURE REVIEW

A hardware based addressing scheme was proposed which uses the MAC address of a device to assign the unique IP address to the node. This works perfect for the addresses IPV6 addresses. But ninety percent of the nodes still use IPV4 addresses and in these addresses the no of bits are smaller than the MAC address. The solution used is hashing the MAC address to fit in the address suffix. But this also includes random choice of address and does not guarantee a collision free address allocation [2].

A new addressing scheme called as duplicate addressing scheme was proposed. In this protocol, every joining node randomly chooses an address and floods the network with an Address Request message (AREQ) if the randomly chosen address is already allocated to another node; this node advertises the duplication to the joining node sending an Address Reply message (AREP). When the joining node receives an AREP, it randomly chooses another address and repeats the flooding process. Otherwise, it allocates the chosen address. But the drawback of this method is that it does not take into account network partitions which are abruptly done at any time in the ad hoc networks [3].

A few extensions to duplicate addressing scheme are also proposed. These extensions use hello messages and partition identifiers. A group of nodes changes its partition identifier whenever it identifies a partition or when partitions merge. A protocol based on DAD is also used to solve address collisions in the presence of network merging events. This protocol considers that two partitions are merging when a node receives a Hello message with a partition identifier different from its own identifier [4].

A weak DAD was proposed which uses a unique key and routing protocol in addressing. Every node is identified by its address and a key. The collisions with the other nodes are identified by information from the routing protocol. If some nodes choose the same address and key, however, the collision is not detected. Also in this case the routing protocol structure is changed. Weak Duplicate Address Detection (DAD) protocol requires each node in the network to have a unique key. Weak DAD requires that packets meant for one node must not be routed to another node, even if the two nodes have chosen the same address. This is achieved by using the key information for duplicate address detection .In this approach; the routing protocol related control packets need to be modified to carry the key information. In the weak DAD scheme, the packet can still be misrouted in the interval between the occurrence of duplicate IP addresses in the network and their actual detection [5].

MANET conf was proposed after weak DAD. Two types of address lists are present, first allocated and allocation pending. A joining node asks for an address to a neighbor, which becomes a leader in the address allocation procedure. The leader chooses an available address, stores it on the Allocated Pending list, and floods the network. If all nodes accept the allocation request and positively answer to the leader, then the leader informs the allocated address to the joining node, moves the allocated address to the Allocated list, and floods the network again to confirm the address allocation [5].

Another addressing scheme based on high entropy is used. The first node in the network is called as Prophet chooses an address. Then it assigns address to any node which contacts it randomly. Thus an address assignment tree is constructed. Prophet does not flood the network as a result the network overhead is limited. But this protocol requires large address range than any of the previous protocols to guarantee that no address is repeated. So to avoid duplication mechanism like DAD is required which increases the protocol complexity and overhead too [6]

A Dynamic addressing protocol was proposed. In this each node has its own address set. This node subdivides its available address set with joining node and assigns the joining node with the available address from the address set. This method works perfect for the small ad hoc networks. But in large ad hoc networks the problem occurs when the all the addresses in the address set are being assigned. Then DAP requires the use of DAD in case of merging events which in turn increase the control overhead [7].

3. FILTER BASED ADDRESSING PROTOCOL

A new protocol is developed which automatically configures addresses using a Filter based approach. It uses two types of filters first is the bloom filter and second is the sequence filter. The bloom filter is used as a partition identifier and sequence filter is used as a storage filter used to store the unique IP addresses. Bloom filter is a data structure which contains n bits. This n bit vector is composed of set of A= {a1, a2…an}.At first all the bits are set to zero. Each element is then hashed by each of the hash functions. Any kind of hashing system can be used like MD5 or a lookup table method. The output represents a position to be set as 1 on the n-bit vector. This hash of the filter is used as a partition identifier which is unique for all the nodes present in a single partition. Here usage of hash filters instead of random numbers reduces the probability of address collisions. This helps to reduce the address collisions with less amount of control overhead in partition merging events. This hash of the filter which is the partition identifier is periodically advertised in the network and thus partitions are detected. The sequence filter compacts the addresses and stores them in a sequence. The first address in the filter is called as initial address. It concatenates this address with an r-bit vector where r is the address range defined by the network suffix. Here a term named ‘delta’ is used. This delta gives the distance between the initial address suffix a (0) suffix and current element suffix which is denoted by a (i) suffix. If the bit is 1 then the chosen address is already present in the address filter and if the bit is 0 then the address is not present in the address filter and it can be allocated to other node requesting for the address.

In the proposed addressing method network prefix of 254 addresses is defined. The nodes in the network randomly choose addresses in the network at first. Whenever the new node joins the network selects an IP address randomly. Then it calculates the delta a. If delta position is found out to be 1 then the address is being used by some other node for communication. If the position indicates 0 then the address is available and the new node can choose the address and further use for communication. This method decreases the control overhead, increases the packet delivery ratio, decreases no of message drops.

By the use of filters the nodes are dynamically assigned IP addresses. The protocol also takes into consideration the partition and merging events which are prominent or very usual in ad hoc networks. The control over head is reduced. Number of message drops is also reduced. Delay is reduced as the whole IP address has not to be checked. By the use of sequence filter checking of the delta position is to be done. If it is ‘1’ the IP address is already assigned and if it is ‘0’ then the IP address is not used and can be assigned to any of the node [9].

4. SIMULATION RESULTS

The tool used for simulation is Network Simulator 2.34. NS2 uses two different languages for simulation namely OTcl and C++.NS2 combines these two languages in a proper manner. C++ is a compiled programming language and NS2 is the interpreted programming language. In C++ the changes take place slowly but running of the code is really fast. Opposite is the case with OTcl language. Thus NS2 combines both of them and forms an efficient tool for network simulation. The executable command used in NS2 is 'ns'. The variables which are declared in OTcl are called as handlers which are mapped to object in C++.These handlers generally do not contain any kind of functionality but the actual function like sending and receiving packets is defined in the object mapped in C++. The interfacing or linking of C++ and OTcl is done through tclcl. This tclcl is a inbuilt directory which contains the code to interface the interpreter which is the OTcl and the backend section coded in C++.NS2 uses a different tool show the simulation results. They are seen in the separate utility called as 'Network Animator i.e. NAM. If the results are to be obtained in the form of graph NS2 has a different utility named as Xgraph. The above figure gives a basic idea of architecture of NS2.It shows C++ linkage to OTcl through TclCL. After simulation a trace file is generated. Depending on the results we actually see the simulation in the NAM window which is a kind of animation. The graph is plotted in Xgraph window. Below are the simulation results

Figure1 gives a scenario of simulation in ns2.The window displayed is nam window i.e. the network animator window. As seen in the below figure there are twenty nodes present, there sources and three destinations. The simulation window is of 500 seconds. Each node is sending Hello messages at respective instant.

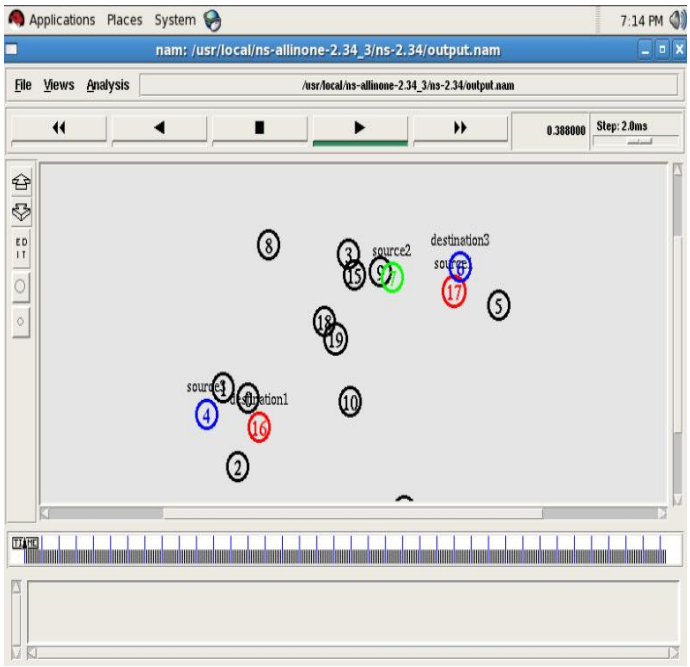

Fig 1: NAM window

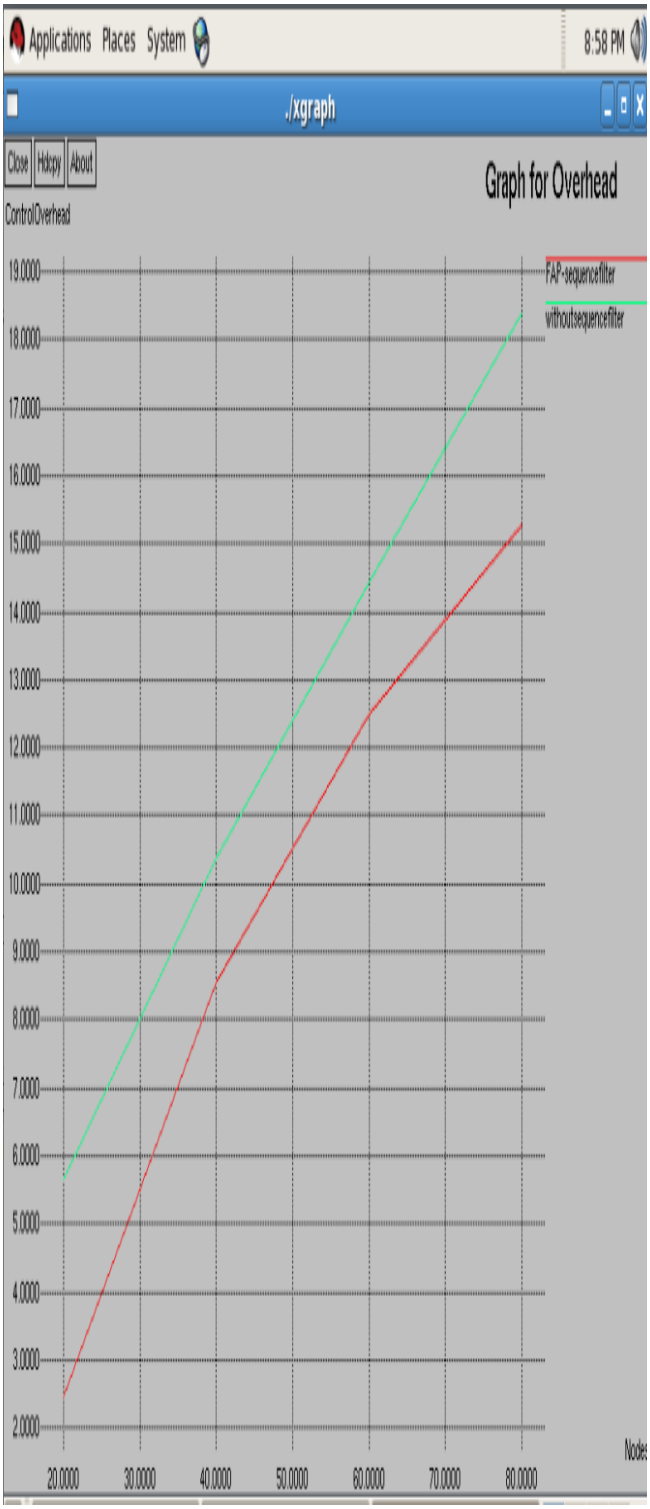

Fig 2: Control overhead v/s number of nodes.

The above figure shows the graph of control overhead v/s number of nodes. In comparison the FAP without a sequence filter which is the basic aodv protocol. Clearly the figure shows that the overhead is less when we consider the protocol with the use of sequence filters.

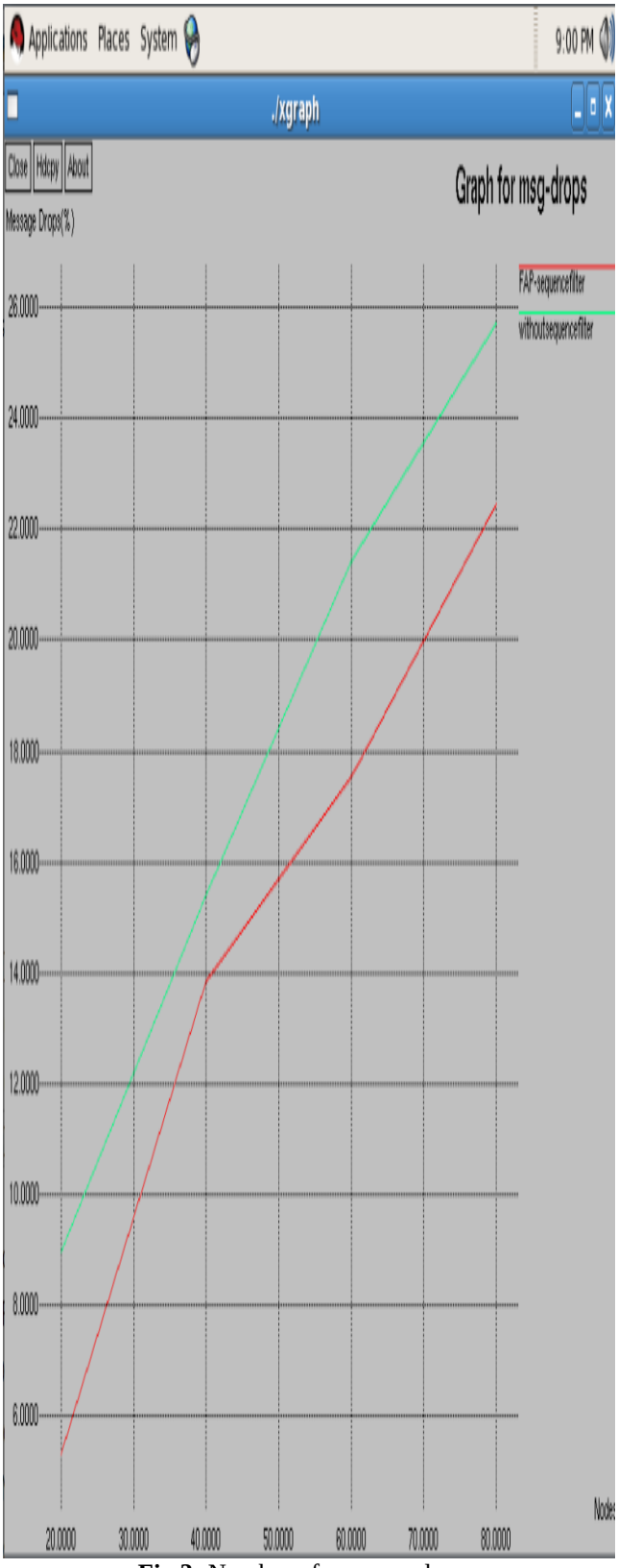

Fig 3: Number of message drops

The above figure shows the number of message drops. Here also the comparison of basic AODV protocol and Filter based addressing protocol is made. The figure clearly shows the number of message drops is less in the proposed protocol as compared to the basic protocol without a filter.

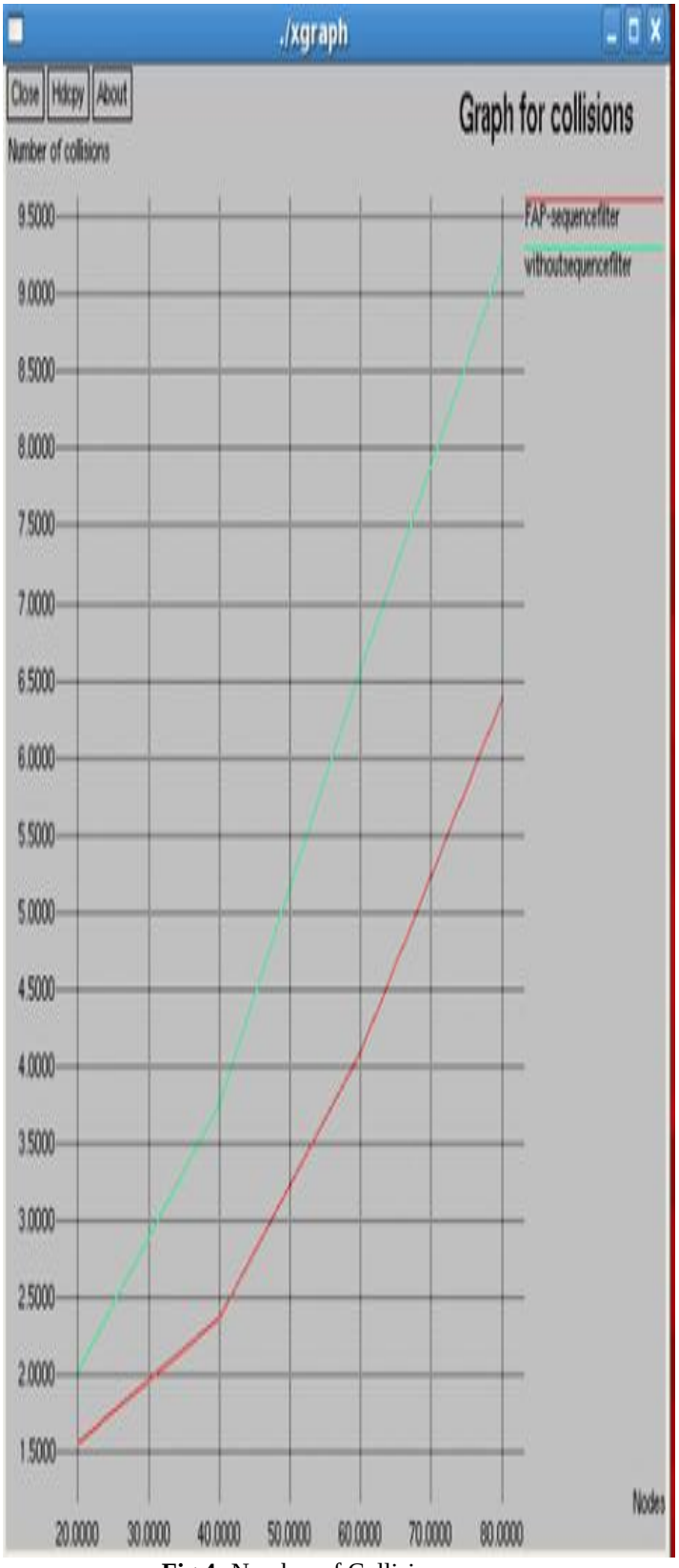

Fig 4: Number of Collisions.

From the above figure it is clear that the number of collisions is less when the protocol is implemented with the filter based concept instead of just the AODV implementation.

5. CONCLUSIONS

Ad hoc networks are formed for the purpose only. Once this purpose is completed the connection is terminated.

Ad hoc networks are infrastructure less networks with lack of central point of contact. The nodes in the network dynamically change their topology hence addressing in such networks is a key issue. In this paper a filter based addressing scheme is implemented. The nodes in the network frequently suffer partition and merging events. To detect these events a filter signature is used instead of random numbers which further adds to the robustness of the protocol. The simulation is carried out in Network simulator2.The graphs of number of message drops, control overhead and numbers of collisions are plotted. It can be clearly seen that the protocol with the use of filter is better than the protocol without the use of filter.

ACKNOWLEDGMENTS

Motivation to do something is of vital importance to achieve success. Authors acknowledge all the experts whose experience and motivation has helped them in the proposing the above mentioned work. Authors also express their regards to the institution for the help provided during the research work.

REFERENCES

[1]. Abulshah,Ashfaq Khokhar,and Mohsen Guizani,"A Survey of Secure Mobile Ad hoc Routing Protocol",in IEEE communications surveys and tutorials,vol 10,no 4,fourth quarter 2008,pp 78-93.
[2]. B.Parno,A.Perrig,and V.Gligor,"Distributed detection of node replication attacks in sensor networks,"in Proc.IEEE
[3]. Symp.Security Privacy,May 2005,pp.49-63.
M. Fazio, M. Villari, and A. Puliafito, "IP address autoconfiguration in ad hoc networks: Design, implementation and measurements," Comput. Netw,vol. 50, no. 7, pp. 898–920, 2006.
[4]. N. H. Vaidya, "Weak duplicate address detection in mobile ad hoc networks," in Proc. 3rd ACM MobiHoc, 2002, pp. 206–216.
[5]. S. Nesargi and R. Prakash, "MANETconf: Configuration of hosts in a mobile ad hoc network," in Proc. 21st Annu. IEEE INFOCOM, Jun. 2002, vol. 2, pp. 1059–1068.
[6]. H. Kim, S. C. Kim, M. Yu, J. K. Song, and P.Mah, "DAP: Dynamic address assignment protocol in mobile ad-hoc networks," in Proc. IEEE ISCE, Jun. 2007, pp. 1–6.
[7]. Deke Guo,Member IEEE JieWu, Fellow IEEE Honghui Chen, Ye Yuan, and Xueshan Luo;" The Dynamic Bloom Filters", IEEE transactions on knowledge and data engineering, vol. 22, no. 1, January 2010,pp-120-132.
[8]. H. Zhou, L. Ni, and M. Mutka, "Prophet address allocation for large scale MANETs," in Proc. 22nd Annu. IEEE INFOCOM, Mar. 2003,vol. 2, pp. 1304–1311
[9]. Natalia Castro Fernandes, Marcelo Duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte", An Efficient and Robust Addressing Protocol for Node Auto configuration in Ad Hoc Networks", IEEE transactions on networking, vol. 21, no. 3, june 2013 p-p 845-856.