Biodiversity:
A Security Approach for Ad Hoc Networks

Jennifer Jackson, Sadie Creese, Mark S. Leeson
University of Warwick
Coventry, UK

Abstract— **Maintaining an adequate level of security in computer networks is a co-evolving process between improved security techniques and ever more sophisticated attack methods. Our appetite for new technologies shows no abating, evidenced most recently by the smartphone market. Malware continues to be a growing problem and saturation times are becoming so rapid that a continued reliance on signature based protection is becoming impractical as a strategy. We urgently require techniques which enable us to adapt to, and be tolerant of, malicious activity, even if it is an entirely new form of attack, to achieve resilience where otherwise our security fails. Ecology research has found that the impact of disturbances to a community, such as the spread of certain types of viruses, can be reduced by a greater level of biodiversity. There are similarities between dynamic ad hoc networks and natural communities due to their movement and short range communication patterns. We explore here whether biodiversity might offer a security strategy for ad hoc networks.**

***Keywords:** adaptability; computer network defence; disturbances; ecology; malware; resilience; tolerance; wireless networks*

I. Introduction

Maintaining an adequate level of security in computer networks is a co-evolving process between improved security techniques and ever more sophisticated attack methods. According to Symantec's security threat report, in 2009 75 percent of enterprises surveyed experienced some form of cyber attack [1]. Cyber crime and the proliferation of malware continue to be a serious threat. According to Kaspersky, new malware grew exponentially every year from 2003 to 2008, and although tapering off in 2009 with improved combined defence mechanisms, this still amounted to approximately 15 million new reported cases [2]. Malware writers are believed to target systems following three criteria: 1) the system is widely used, 2) has good quality documentation, and 3) is unsecure or has documented vulnerabilities [3]. This is evidenced in the large number of malware applications targeting computers running the Microsoft Windows operating system and its widely used suite of Office tools. The trend is also apparent with mobile phones where the Symbian operating system has been targeted. More recently the proliferation of social networking using Web 2.0 to facilitate communication has led to a large rise in Web 2.0 specific malware. In 2007, when Web 2.0 was in its infancy, 10,000 new malicious malware programs were reported, and in 2008 this figure rose to 25,000 [4]. Our appetite for new technologies shows no abating, evidenced most recently by the smartphone market. Information infrastructures, and increasingly ad hoc networks [5], pervade our lives, underpin our critical national infrastructures, our cars, our workplaces, our homes and increasingly our social lives. Malware continues to be a growing problem and saturation times are becoming so rapid that a continued reliance on signature based protection is becoming impractical as a strategy. We urgently require techniques which enable us to adapt to, and be tolerant of, malicious activity, even if it is an entirely new form of attack. We need resilience in the presence of malign environments and agents, as well as benign failures.

Research within the field of ecology has found that the spread of certain types of viruses can be reduced within a community by having a greater level of biodiversity [6, 7]. Biodiversity is the range of plants, animals, insects and other organisms present in a particular ecological community or system. Biodiversity promotes resistance to disturbances towards the functioning of the ecosystem, not just from viruses, but from changing environmental conditions such as droughts [8]. The biodiversity concept does not try to eliminate these disturbances within the ecosystem, but to tolerate them and prevent them from causing immediate wide spread devastation.

There are similarities between ad hoc networks and natural communities. In the natural environment, for example, animals may move around their surroundings coming into contact with each other, whilst ad hoc nodes often move around forming temporary links with other nodes. Mobile devices, such as smartphones and laptops, can already participate in temporary ad hoc networks and tend to move around with their user following similar patterns to the movement of humans. Some types of ad hoc networks may move in complete communities or remain static, such as sensor networks, where only communication with local nodes is undertaken to gather and disseminate information and observe changes within the environment. Such patterns can be found in nature with herds of animals or flocks of birds or even in a static landscape with growing plants. We explore here whether biodiversity could provide a new type of security strategy designed to provide ad hoc networks with an ability to tolerate disturbances caused by security threats such as malware.

Section 2 of this paper reviews research regarding the use of biodiversity within computer networks. Section 3 defines the role of biodiversity as a security approach in ad hoc networks by exploring biodiversity from an ecological perspective, and Section 4 presents our conclusions and future work directions.

This work was supported in part by the Complexity Science Doctoral Training Centre at the University of Warwick under EPSRC funding.

978-1-4244-9906-9/11/$26.00 ©2011 IEEE

II. Biodiversity in Computer Networks

In the 1970s N-version programming was proposed within the field of fault tolerance to increase the reliability of systems that used software. It was known that identical software running on independent systems would fail in exactly the same way with the same inputs, so the idea was therefore to create N-versions of the software. Since then the concept of increased diversity within computer networks has expanded, with the majority of research focused upon applications such as improving communications [9-11], avoiding security attacks [12-16], designing fault tolerant systems for harsh environments [17-20] improving test simulations [21], and in developing enabling technologies to support such concepts [22]. This literature regarding diversity within computer networks highlights that there are many dimensions to diversity that need to be considered. The diversity wheel in Fig. 2 gives an appreciation of the many dimensions and layers which are being explored. A biological perspective on diversity, in the form of biodiversity, has largely been overlooked. In 1997, Forrest [23] touched upon this concept by recognising that diversity is an important source of robustness in biological systems, and its beneficial effects in computing systems had been ignored. Biodiversity, however, cannot be considered in isolation and requires an ecological perspective to understand its interactions and effects on the system. In 2008 Forrest co-authored a paper suggesting that malware could be considered from an ecological perspective [24] but there is still a large gap in understanding the actual benefits of biodiversity as a security mechanism. There has been very little research into the underlying theory and its impact on networks. In 2006 an expert panel came together to discuss the topic of diversity and its use as a computer defence mechanism [25]. They argued that not enough is known about diversity to make it useful for computer security despite continuing to surface as a proposed solution. A number of open research questions were discussed such as diversity definitions, its dimensions and its metrics, the strength of security protection offered by diversity, the benefits and the costs. Our research goal is to understand how biodiversity might offer effective security, and to be able to compare the impact of varying strategies. We approach this initially by application to ad hoc networks, although our methodology is likely to be more generally applicable. The remainder of this paper will begin to define the role of biodiversity as a security approach in ad hoc networks from an ecological perspective with fundamental analogies between ecology and the ad hoc network environment.

III. The Role of Biodiversity as a Security Approach in Ad Hoc Networks

A. *An Ecosystem Perspective of an Ad Hoc Network Environment*

The role of biodiversity as a security mechanism can be considered by understanding the factors that enable biodiversity to work within nature. The concept of biodiversity however, cannot be considered in isolation, and requires an ecosystem perspective following ecological principles at different scales. Ecology research has found that an important benefit of biodiversity is its resilience against disturbances to the current functioning of the ecosystem. The resilience of an ecosystem is the amount of disturbance that an ecosystem can withstand, and disturbances that happen within the tolerated range usually result in little long term change in ecosystem dynamics. Events outside this tolerated range, however, can change ecosystem function. Ecosystem function and resilience to disturbances is maintained by biodiversity at the individual (I) scale through genetic diversity, at the community (C) scale through species and functional diversity, and at the ecosystem (E) scale through ecological diversity.

If an ad hoc network, together with its user and application environment, is regarded as an ecosystem then security attacks can be thought of as destructive disturbances at the individual, community, or ecosystem scale affecting the functioning of the services provided by the network. In an ad hoc network the individual scale would comprise the individual nodes and would be concerned with application software, protocol stacks, physical hardware, and behavioral characteristics. The community scale would comprise communities of nodes forming part of a network, or a complete network. This scale would be concerned with topology and node type distribution, data flow and mobility, and community level behaviors. The ecosystem scale would comprise multiple clusters of nodes or multiple networks and interactions between them. It would also comprise the physical application environment and human user beneficiaries. This scale would be concerned with the over-all functioning of the network together with its interaction environment and the beneficial services provided such as an electronic health care service or an environmental monitoring service. By applying biodiversity strategies at different scales, it is hypothesised that the destructive effects arising from security attacks can be counterbalanced with the constructive effects of biodiversity to maintain ecosystem function and services, and hence increase over-all resilience. See Fig. 1.

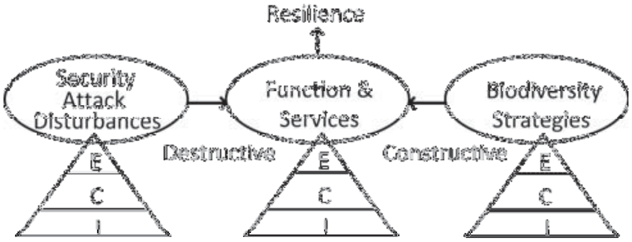

Figure 1- Ecosystem Resilience Model for a Computer Network

B. *Disturbances and Security Attacks*

Within an ecosystem it is necessary to distinguish between the natural disturbance regime [26] and a single disturbance event. A natural disturbance regime describes the pattern of disturbances that shape an ecosystem over a long time scale. Ecosystems themselves are dynamic, and natural changes to the functioning of the ecosystem are created by environmental effects and changes in biodiversity. Within an ad hoc network environment, technological advances, trends in user habits, business markets, and application areas will contribute to natural changes in ecosystem function. A single disturbance is an event of intense stress occurring over a relatively short period of time causing large changes in the ecosystem.

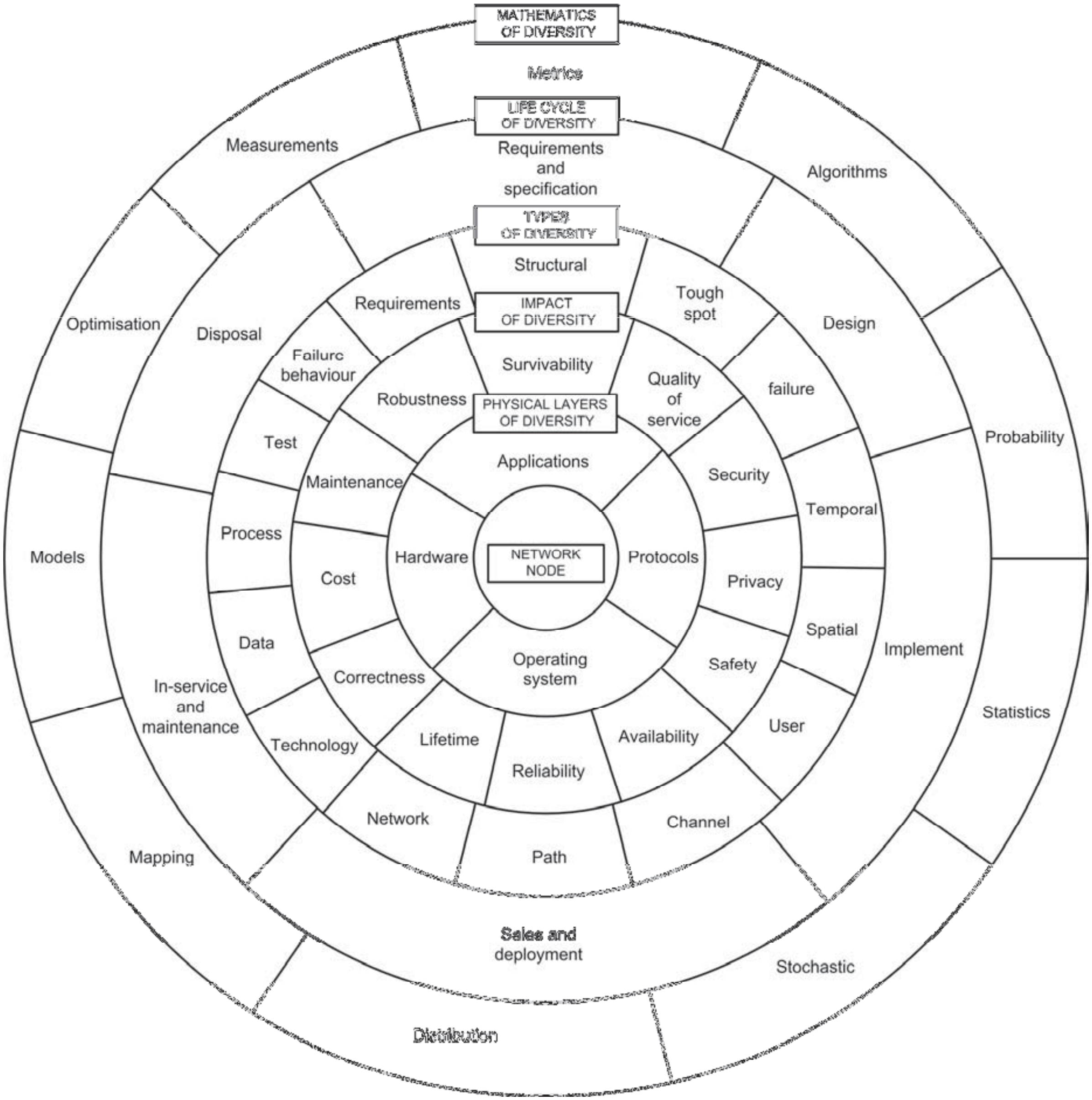

Figure 2 – The Diversity Wheel

Examples of some natural single disturbance events include tornadoes, disease epidemics, droughts and fires. Within an ad hoc network environment security attacks can be thought of as single disturbance events. These security attacks can be initiated from any of the three scales of the ad hoc network environment to create destructive disturbances at varying speeds and severity depending upon the specific attack. Table I shows an example set of security attack disturbances and the effects they have on the function and services of an ad hoc network at the three different scales [27-30]. Disturbances created by individual nodes or within the community can directly affect the function and services at the individual or community scales (X), and in some cases if the tolerance at each scale is surpassed, effects can ripple through the scales impacting the over-all ecosystem function and services (O). Attacks such as a denial of service can be directed at a specific node, operating system, or network resulting in a lack of available resources to send and receive data. This can reduce availability for network communication or cause excessive delays. Impersonation attacks, where a node assumes the identity of another node, can compromise data and entire sections of the network infrastructure, and distort routing behaviours. The impersonator may be able to gain access to encryption keys, authentification information, and reconfigure the network so that other attackers can join in.

TABLE I SECURITY ATTACK DISTURBANCES AND THEIR EFFECTS ON FUNCTION AND SERVICES

	Effects on Function and Services														
	Individual									Community					Ecosystem
Security Attack Disturbances	Operation of node slows down	Application or protocol software stops working	Damage to stored data	Complete node shutdown	Increase in received messages	Increase in transmitted messages	Unable to transmit messages	Unable to receive messages	Unauthorised collection of data	Reduced availability for network communication	Excessive network delays	Increased or bursts in network traffic	Sections of network infrastructure compromised	Distorted routing behaviours	Reduction in Ecosystem services
Denial of Service	X				X		X			X	X				O
Impersonation									X				X	X	O
Message modification								X	X	X	X			X	O
Message replay					X					X		X			O
Wormhole/Blackhole								X		X	X			X	O
Active worms	X		X			X				X		X			O
Passive worms	X		X												
Viruses	X	X	X	X	X	X	X	X		X		X			O
Physical destruction of node				X						O					O
Distributed Denial of Service	X				X		X			X	X	X		X	O
Eavesdropping									X						
Trojans	X				X		X		X						
Spyware									X						
Physical destruction of community										X					X
Destruction of working environment															X
Removal of human beneficiaries															X

The *message modification attack* may route messages away from its intended destination and change the routing behaviour leaving the recipient unable to retrieve data, making the network appear unavailable. Some communication protocols allow data to be retransmitted if no acknowledgement of receipt is received causing delays in the eventual transmission of the data. During a *message replay attack* messages are stored and then later distributed on the network using up resources making them unavailable for normal use. A node generating a *black hole attack* can suck data in from neighbouring nodes by announcing that it is free to forward messages without ever doing so, and hence affecting normal routing behaviour and the reception of messages. *Wormholes* on the other hand can prevent data from arriving at its intended destination by tunnelling them to another location in the network, and then retransmitting them. *Active worms* and certain *viruses* replicate and forward themselves as fast as possible increasing the level of traffic on the network, using up resources, and leaving the network unavailable for normal use. This increased traffic is noticeable over short time periods as the worms and viruses quickly spread throughout the network. Viruses tend to cause more damage to network nodes leaving them unable to operate or communicate within the network. *Passive worms* and certain types of other viruses are embedded within normal data traffic so although their propagation speeds are slower than active worms or other viruses, they create no obvious change in the behaviour of the network. The *physical destruction of a node* can often be tolerated at the community level, however if the number of nodes destroyed surpasses a threshold there will be a reduction in resources reducing communication availability. A *distributed denial of service attack* can be targeted at an individual node or network by flooding them with traffic, but additionally the attacker nodes may refuse to forward data packets reducing the number of nodes available to provide the network with resources and hence reducing the availability for network communication. A passive technique such as *eavesdropping* listens to passing messages without disturbing the normal flow of data causing little or no change in behaviour at the community scale. *Trojans* and *spyware* are usually installed by mistake hidden within genuine applications which then access and slowly exfiltrate personal data from a node without affecting the functioning of the network. Some Trojans however are used to perform other types of attacks such as distributed denial of service. The *physical destruction of a community* can not only reduce network availability but could also affect the services of the ad hoc network. Some security attacks can create ecosystem scale disturbances directly, such as a physical *destruction of the working environment* or the *removal of human beneficiaries*. Other examples might relate to loss of trust in a brand or identity, perhaps resulting from a malicious misinformation campaign, unexpected stock market activities, extreme events, conflict, or new regulation. Whilst others are created indirectly through destructive disturbances at lower scales subsequently impacting higher scales. Active worms, for example, can quickly create disturbances that ripple up through the scales to reduce the network function or service at the ecosystem scale within a short period of time.

C. *Biodiversity Scales, Measurements and Classification*

The application of biodiversity strategies at various scales within an ad hoc network environment, requires us to consider the definition and measurement of biodiversity at these three scales [31]. It is also necessary to define a three scale ad hoc network classification system to enable biodiversity strategies to be defined and measured as shown in Table II. Within the field of Ecology, diversity within species is measured at the individual scale which often requires a genetic approach to evaluate detailed differences between individuals. Genotypes are used to determine the actual set of genes carried by an individual when measuring genetic differences. Phenotypes are used to measure the observable characteristics and traits coded for by those genes. Individuals with the same genotype rarely look or act the same because phenotype appearance and behaviour are modified by environmental and developmental conditions. Similarly, individuals that look alike do not necessarily have the same genotype, so it is important to consider both of these different types of classifications. Within an ad hoc network environment biodiversity measurements will need to ascertain detailed differences between ad hoc nodes and therefore classification at this scale may require two methods; one to provide a genotype classification of the software and hardware structure of an individual node, and another to provide a phenotype classification of traits or behavioural characteristics of an individual node such as its mobility pattern.

At the community scale, quantification of the number of different species is often measured, termed species diversity, together with their distribution. The classification of species in natural systems is usually via a taxonomy approach using a hierarchical branching structure with various kingdoms defining the top level such as the animal kingdom. This type of hierarchical structure allows for the measurement of diversity not just at the species level but also at higher levels so that different granularities of diversity can be measured within a community. Also at the community scale functional diversity is used to measure differences by categorising species into groups that perform similar ecosystem processes. Functional groups for example are often split into primary producers (plants), herbivores (eat plants), carnivores (eat meat), omnivores (eat plants and meat), and detrivores (live on organic matter). The classification of an ad hoc network environment at the community scale therefore requires two methods; one to provide a species taxonomy classification such as the classification of ad hoc node types according to device product lines and form factors, and another to provide functional classification such as the classification of ad hoc node types according to the production and consumption of resources.

At the ecosystem scale the diversity of communities, geographical regions or complete ecosystems are measured. It is at this scale that differences between two or more communities or geographical regions are also considered, and sometimes diversity changes within one region is measured over time. Within an ad hoc network environment this would translate to measuring the diversity of node clusters, the diversity between clusters of a large network, the diversity between networks, the diversity between ad hoc environments, and the diversity changes over time. Measuring only differences between communities such as node clusters or networks over space and time involves comparing species and functional diversity measurements and for this no additional classification system is needed. However ecosystems and geographical regions include not only communities, but also their physical environment. For an ad hoc network system this would include the application environment including any possible human user beneficiaries, regulation, market forces, social norms etc. To measure these ecosystem scale differences the classification of the application environment is required.

TABLE II BIODIVERSITY SCALES, MEASUREMENTS, AND CLASSIFICATION

Biodiversity Scale	**Ad Hoc Network Environment**	
	Biodiversity Measurements	**Classification**
Individual: Genetic Diversity	Detailed differences between ad hoc nodes.	Genotype: Classification of software & hardware composition. Phenotype: Classification of behavioural traits & characteristics.
Community: Species & Functional Diversity	Quantification of different ad hoc node types, their distribution and topology.	Species: Taxonomy classification of ad hoc node types according to device product lines and form factors. Functional: classification of ad hoc node types according to similarities in their functional processes.
Ecosystem: Ecological Diversity	Diversity of node clusters. Diversity between clusters of a large network, between networks, or between application environments. Diversity changes over time.	Environment: Classification of the ad hoc network application environment.

D. Ecosystem Resilience and Biodiversity Strategies

The resilience of an ecosystem is the amount of disturbance that it can withstand and is closely linked with the level of biodiversity within that ecosystem. The natural level of ecosystem biodiversity has evolved through the natural disturbance regime over a specific range of time and space. Therefore current disturbances created within this range can be tolerated, and the greater the range of tolerance, the greater the resilience of the ecosystem. Increasing the range of tolerance can be achieved by replicating ecological processes through natural disturbances and increasing biodiversity across all scales. This means that applying biodiversity strategies is far more than just increasing the number of different species. Resilience depends upon diverse individual population attributes to create different response dynamics, the organisation of species among functional groups, diverse spatial patterns and environments, and the scaling of strategies in time and space [32].

There are two main categories of biodiversity strategies occurring within the natural environment. Strategies that are *natural* happen normally without intervention, and strategies that are *induced* are artificially created to improve the current ecosystem function and resilience. These biodiversity strategies used within natural systems can be translated into the context of ad hoc networks along with their perceived potential benefits as given in Table III. At the individual scale natural biodiversity can come from the birth and death of individuals by altering the quantity and distribution of different species. Within an ad hoc network environment this may mean nodes naturally entering or leaving the network at different time and spatial scales, or it may mean the introduction of new technology, new makes and models coming out onto the market, or the removal of old technology. This in turn will have the benefit of changing the density and distribution of nodes in the network altering network resources and availability for communication. Natural biodiversity at this scale can also result from breeding where genes are exchanged or mutated creating a newly diverse individual. Within an ad hoc network environment the exchange or modification of software, particularly in the case of open source software will naturally encourage changes in configuration and continual addition and subtraction of functionality and data. This will have the benefit of increasing the variation of nodes and reducing the vulnerability to particular disturbances. Another natural biodiversity strategy at this scale can result from the effects of individual migration from one region to another shifting the biodiversity distribution. Within an ad hoc network environment the movement of nodes through mobility patterns or long term relocation can aid the exchange of software, and also change biodiversity patterns over space and time. Induced strategies at the individual level involve genetic modification or forced breeding to retain or remove specific characteristics or vulnerabilities for the benefit of the individual, community, or ecosystem. Within an ad hoc network environment this means the modification of software and hardware structure or characteristics to create additional variation within or between node types. Creation or modification may include the generation of specific beneficial nodes, or specific behavioural strategies for the exchange or modification of software. This allows nodes to be modified in a beneficial manner through static or dynamic strategies in space and time to increase resilience or aid response and recovery to disturbances.

At the community scale natural biodiversity can originate from evolution and natural selection through competition and survival of the fittest, which in turn provides ecosystem resilience and a greater range of services and benefits. For ad hoc networks, this may mean natural competition of node types with selection based upon human requirements, fitness for purpose and vulnerability to digital viruses. This process can produce more beneficial node types, increase their density and improve network function and services. Two of the most important induced biodiversity strategies at the community level can be developed from ecological research. The first strategy comes from the discovered importance of community structure and diverse species distribution, and their role in the over-all response of the ecosystem to disturbance [32]. Strategies that ensure complementary species distribution over space and time are likely to increase the range of tolerance to disturbance. Within an ad hoc network environment strategies to ensure node types with complementary attributes that are distributed appropriately within the local network community can therefore provide a greater range of community response to disturbance. The second strategy comes from the discovered importance of the complementary use of resources by functional groups which can provide a greater flow of ecosystem services [32]. For example plants that root at different depths and grow or disperse seeds at different times of the year increase ecosystem productivity. This may also be true in ad hoc network environments, for example when data is stored and dispersed via different methods or times, increasing the flow of services. Other community level induced strategies include practical methods for the addition or subtraction of species to rebalance the level of biodiversity within the community such as culling, introducing predators or competitors, and changing the density distribution or location. Within an ad hoc network environment this could mean imposing limits on the number of node types in a network community, introducing strategically placed sacrificial or beneficial nodes, creating competition strategies, and methods for changing the density and location or communication between nodes. Such strategies can improve over-all network resilience through static or dynamic strategies in space and time.

At the ecosystem scale natural biodiversity strategies are concerned with small environment changes or disturbances which alter the conditions in which the community operates. This can alter the productivity of the ecosystem or the suitability of certain species and can sometimes drive a change in biodiversity. Within an ad hoc network these environment changes can come from physical obstructions of new objects or weather effects or changes in location of the community e.g movement of a body sensor network. Induced biodiversity strategies at the ecosystem scale include deliberate changes in the environment such as providing extra habitat or resting sites and creating areas high in environmental diversity to retain and attract species diversity.

TABLE III BIODIVERSITY STRATEGIES AND THEIR PERCEIVED BENEFITS

	Ad Hoc Network Biodiversity Strategies	Function and Resilience Benefits
Individual	**Natural:** 1.Birth and death: Introduction or removal of nodes. 2.Breeding : Exchange or modification of software. 3.Migration: Mobility pattern of a node. **Induced:** 1.Genetic modification: Modification of software/hardware structure & characteristics. 2.Forced Breeding: Creation of a specific beneficial node type, or variation of types, or strategies for the exchange or modification of software.	**Natural:** 1.Alters the density of nodes and resources available for communication. 2.Increases variation of nodes and reduces vulnerability to disturbances. 3.Changes node density and biodiversity levels over space and time. **Induced:** 1.Increases variation of nodes and reduces ecosystem vulnerability to particular disturbances. 2.Nodes can be modified in a beneficial manner through static or dynamic strategies in space and time. This can increase resilience or aid response and recovery to disturbances.
Community	**Natural:** 1.Evolution & natural selection: Natural competition of node types with selection based upon human requirements fitness for purpose, and vulnerability to digital viruses. **Induced:** 1.Complementary species: Strategies to ensure node types with complementary attributes are distributed appropriately within the local network community. 2.Complementary resource usage: Strategies to ensure functional groups present within a community are complementary in their use of resources. 3.Culling: Limit the number of node types in a community. 4.Predators, competitors, or pathogens: Introduce beneficial nodes to eliminate attacker nodes or restrict dominating node types. Introduce competition strategies between node types. 5.Sacrificial species: Introduce a sacrificial node type. 6.Attractor species: Introduce a node type to attract beneficial nodes. 7.Density: Change the density of certain node types, employ type rotation or intermixing, replace with less vulnerable types. 8.Location and contact: Strategies to avoid nodes with similar vulnerabilities.	**Natural:** 1. Produces more beneficial node types, increases their density and improves network function and services. Can also reduce dominant node types and vulnerability of the ecosystem. **Induced**: 1.Greater range of community response to disturbance. 2.Greater flow of ecosystem services. 3.Can increase diversity in network communities and reduce vulnerability to particular disturbances. 4.Reduces dominant node types, but can also improve services through competition and adaptation. 5.Provides an easy target node which has no benefit or function to the network to fool or stop the attacker. Can be re-programmed after sacrificed. 6.Beneficial node types join the network as a result, improving services and increasing resilience. 7. Improves biodiversity and hence network resilience through static or dynamic strategies in space and time. 8.Reduces virus transmission or unbeneficial software and improve network availability through dynamic and static strategies in space and time.
Ecosystem	**Natural:** 1.Environment changes: Physical changes of or within the ad hoc network environment. **Induced:** 1.Environment & habitat changes: Replicate a desired natural disturbance regime for the ad hoc network environment 2.Biodiversity belts: Create biodiversity belts around homogeneous node communities. 3.Increase available nutrients: Increase available resources within the ecosystem. 4.Provide incentives and benefits: Create incentives and benefit sharing schemes	**Natural:** 1.Alters the suitability and productivity of the current network function giving rise to a required change in biodiversity mix. **Induced:** 1. Small scale disturbances to encourage diverse node types and increase the range of tolerance and hence resilience. 2. Provides segregation of vulnerable network communities. Offers some protection against external community disturbances. 3. Can increase the amount of data flow or availability for communication. 4. Can attract node types to an area and provide additional services and benefits.

Within an ad hoc network, deliberate changes in the environment can force increased diversity and hence ecosystem resilience; biodiversity belts can provide segregation of vulnerable network communities and offer some protection against external community disturbances. The induced strategy of increasing the availability of nutrients can increase the energy flow within an ecosystem. For an ad hoc network environment this may mean increasing the availability of resources and hence increasing the amount of data flow or availability for communication. The induced strategy of providing incentives and benefit sharing schemes can involve human beneficiaries. Within the ad hoc network environment this could include incentive strategies for nodes, communities or end users through policy making or other ecosystem scale schemes. These schemes can attract node types to an area to provide additional services and benefits.

E. Multiscale Modelling of Biodiversity Strategies

Modelling the ad hoc network environment and biodiversity strategies at the scales discussed across space and time requires a multiscale method to capture complex interactions and emergent effects. Agent based modelling is a bottom up approach with the ability to simulate such complex effects and predict emergent behaviors not expected from traditional mathematical models. Agents within the model usually have some degree of self-awareness, intelligence, autonomous behaviour, knowledge of the environment and other agents, and can adjust their own actions in response to environmental changes. Within an ad hoc network environment the agents will become the nodes, programmed to exhibit structure and behaviours representative of particular node types. The level of detail programmed into each node depends on the type of strategies being simulated, the required realism of the model, computation limitations and the methods used to generate the model. To include structural and behavioral genetic diversity at the individual level requires sufficient detail to capture subtle differences in node responses under different security attacks.

IV. Conclusion and Future Work

There is a large gap in understanding the benefits of biodiversity within computer networks and its underlying theory, particularly as a security mechanism. Ad hoc networks have similarities to natural communities making them good candidates for studying this aspect. Regarding ad hoc networks as ecosystems means that security attacks can be thought of as single disturbance events affecting the functioning of the services provided by the network. We hypothesise that the destructive effects from security attacks can be counterbalanced with constructive effects of biodiversity strategies to maintain services and increase over-all resilience. To apply and measure the effectiveness of biodiversity strategies, a three scale ad hoc network classification system has been defined. Applying biodiversity strategies within this ad hoc network environment is far more than just increasing the number of different node types. Resilience depends upon diverse individual node attributes to create different response dynamics, the organisation of node types among functional groups, diverse spatial patterns and environments, and the scaling of strategies in time and space. Natural and induced biodiversity strategies have been translated into the context of an ad hoc network environment along with their perceived potential benefits. Such an analogy is needed to enable successful biodiversity methods to be applied to ad hoc networks. This will facilitate future research to establish whether such methods can increase resilience within these networks. We hypothesise that improving resilience in such ad hoc network environments via this multi-scaled approach will improve the quality and reliability of services offered by enterprises in the face of changing security threats. Future research will continue the exploration of ad hoc network biodiversity. Multi-scale simulation techniques, such as agent based modelling, will be employed to capture the complex interactions and emergent effects that the nodes and strategies create. The over-all function of the ad hoc network ecosystem will be combined with the destructiveness of the security attacks to assess the effectiveness of any biodiversity strategy employed to ascertain the global level of security. We will also explore the broader applicability of this approach to other types of system, and investigate methods to measure and compare the relative security benefits.

References

[1] *Symantec global internet security threat report, trends for 2009*, 2010.

[2] E. Aseev, and A. Gostev. "Kaspersky security bulletin 2009. Malware evolution 2009," http://www.viruslist.com.

[3] "Three criteria for malware existence." http://virustlist.com.

[4] S. Tanase, “When web 2.0 sneezes...Everyone gets sick,” *IET Engineering & Technology,* vol. 5, no. 5, pp. 28-29, 2010.

[5] I. Chlamtac, M. Conti, and L. J. J.-N, “Mobile ad hoc networking: Imperatives and challenges,” *Ad Hoc Networks,* vol. 1, no. 1, pp. 13-64, 2003.

[6] R. S. Ostfeld, and F. Keesing, “Biodiversity and disease risk: The case of lyme disease,” *Conservation Biology,* vol. 14, no. 3, pp. 722-728, 2000.

[7] L. J. Dizney, and L. A. Ruedas, “Increased host species diversity and decreased prevalence of sin nombre virus ” *Emerging Infectious Diseases,* vol. 15, no. 7, pp. 1012-1018, 2009.

[8] D. Tilman, and J. A. Downing, “Biodiversity and stability in grasslands,” *Nature,* vol. 367, no. January, pp. 363-365, 1994.

[9] S. Jain, and S. R. Das, “Exploiting path diversity in the link layer in wireless ad hoc networks,” *Ad Hoc Networks,* vol. 6, no. 5, pp. 805-825, 2008.

[10] T. Issariyakul, and V. Krishnamurthy, “Amplify-and-forward cooperative diversity wireless networks: Model, analysis, and monotonicity properties,” *IEEE/ACM Transactions on Networking,* vol. 17, no. 1, pp. 225-238, 2009.

[11] H. Lim, C. Lim, and J. C. Hou, “A coordinate-based approach for exploiting temporal-spatial diversity in wireless mesh networks,” in MobiCom, 2006.

[12] M. G. Bailey, “Malware resistant networking using system diversity,” in SIGITE, 2005.

[13] A. J. O'Donnell, and H. Sethu, “On achieving software diversity for improved network security using distributed coloring algorithms,” in CCS, 2004.

[14] Y. Zhou, Z.-F. Wu, H. Wang *et al.*, “Breaking monocultures in p2p networks for worm prevention,” in Machine Learning and Cybernetics, 2006.

[15] Y. Yang, S. Zhu, and G. Cao, “Improving sensor network immunity under worm attacks: A software diversity approach,” in MobiHoc, 2008.

[16] B. Anckaert, B. De Sutter, and K. De Bosschere, “Software piracy prevention through diversity,” in DRM, 2004.

[17] N. L. Hung, A. R. Jacob, and S. E. Makris, “Alternatives to achieve software diversity in common channel signaling networks,” *IEEE Journal on Selected Areas in Communications,* vol. 12, no. 3, pp. 533-538, 1994.

[18] B. Littlewood, P. Popov, and L. Strigini, “Modeling software design diversity - a review,” *ACM Computing Surveys,* vol. 33, no. 2, pp. 177-208, 2001.

[19] G. Gaiswinkler, and A. Gerstinger, “Automated software diversity for hardware fault detection,” in Emerging Technologies & Factory Automation, 2009.

[20] M. R. Lyu, J.-H. Chen, and A. Avizienis, “Software diversity metrics and measurements,” in Computer Software and Applications Conference, 1992.

[21] B. Nikolik, “Test diversity,” *Information and Software Technology,* vol. 48, no. 11, pp. 1083-1094, 2006.

[22] E. Ipek, M. Kirman, N. Kirman, and J. F. Martinez, “Core fusion: Accommodating software diversity in chip multiprocessors,” in ISCA, 2007.

[23] S. Forrest, A. Somayaji, and D. H. Ackley, “Building diverse computer systems,” in Workshop on Hot Topics in Operating Systems, 1997.

[24] J. R. Crandall, R. Ensafi, and S. Forrest, “The ecology of malware,” in NSPW, 2008.

[25] C. Taylor, and J. Alves-Foss, “Diversity as a computer defense mechanism a panel,” in NSPW, 2006.

[26] S. T. A. Pickett, and P. S. White, *Natural disturbance and patch dynamics*: Academic Press, 1985.

[27] L. Tamilselvan, and D. V. Sankaranarayanan, “Prevention of impersonation attack in wireless mobile ad hoc networks,” *Computer Science and Network Security,* vol. 7, no. 3, pp. 118-123, 2007.

[28] S. Dhanalakshmi, and D. M. Rajaram, “A reliable and secure framework for detection and isolation of malicious nodes in manet,” *Computer Science and Network Security,* vol. 8, no. 10, pp. 184-190, 2008.

[29] M. Hypponen, “Malware goes mobile,” *Scientific American*, November, 2006.

[30] S. A. Razak, S. M. Furnell, and P. J. Brooke, “Attacks against mobile ad hoc networks routing protocols,” in 5th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking & Broadcasting, PGNET, 2004.

[31] A. E. Magurran, *Measuring biological diversity*: Blackwell, 2003.

[32] "Scenarios, volume 2," *Ecosystems and human well-being*, S. R. Carpenter, P. L. Pingali, E. M. Bennett and M. B. Zurek, eds.: Island Press, 2005.