YAPISIZ (AD HOC) KABLOSUZ AĞLARDA GÜVENLİK

Tuncay ERCAN, Samsun M. BAŞARICI, İbrahim ZİNCİR
Bilgisayar Mühendisliği, Yaşar Üniversitesi, İzmir
tuncay.ercan@yasar.edu.tr; samsun.basarici@yasar.edu.tr; ibrahim.zincir@yasar.edu.tr

Özet— Son yıllarda gelişen kablosuz iletişim teknolojileri özellikle kablosuz ağlar alanında yeni seçenekler ve kullanım olanakları ortaya çıkarmıştır. Bu alanlardan birisi de yapısız kablosuz ağlardır. Gelişen teknolojiler her ne kadar büyük fırsatlar sunsa da özellikle ağ güvenliği konusunda büyük sorunlar içermektedir. Yapısız kablosuz ağlar, iki veya daha fazla taşınabilir sunucunun önceden belirlenmiş kurallar ya da yapılar olmadan anlık bir şekilde birbirleriyle sınırlı fiziksel alanlarda bilgi paylaşımını sağlayan iletişim sistemleridir.

Bu tip ağlarda taşınabilir cihazlarla kurulan kablosuz iletişimden kaynaklanan sorunların yanında, ağın standart bir yapısının olmaması sebebiyle sık sık değişen topolojik özelliklerinin sebep olduğu güvenlik sorunları da vardır. Dinamik güncelleme bilgileri ağ kaynaklarını devamlı olarak meşgul etmekte, değişiklikler ile ilgili bilginin geç gelmesi ağda istikrarsızlığa yol açmaktadır. Bu alanda yapılan çalışmaların büyük bir kısmı ortaya çıkan bu güvenlik sorunlarını çözebilmek için kriptoloji, kimlik denetimi ve kimlik doğrulaması, ağa yapılabilecek olası saldırıların keşfi ve karşı önlemlerin alınabilmesi gibi genel savunma yöntemlerini kullanmaktadır. Ancak yapısız kablosuz ağların yapılarından ve anlık olarak ortaya çıkmalarından kaynaklanan özel koşullar genel çözüm yöntemlerinin etkilerinin çoğunlukla sınırlı kalmasına neden olmakta ve yeni yaklaşımlar gerektirmektedir.

Bu çalışmada ilgili güvenlik sorunlarının Yapısız Ağlarda yarattığı sorunlar ve olası çözümler üzerinde durulmuştur.

Anahtar Kelimeler: Ad-hoc, yapısız ağlar, güvenlik, kablosuz ağlar

1 Giriş

Kablosuz ağlar günümüzde bankacılıktan mesaj göndermeye, habercilikten televizyonculuğa kadar hemen her alanda çok yaygın bir şekilde kullanılmaktadırlar. Gelişen teknolojiyle birlikte yaşamın ayrılmaz bir parçası haline gelmiş, günlük hayatın olmazsa olmazları arasına girmişlerdir. Kablosuz ağlar, basit bir yaklaşımla, iki ya daha fazla bilgisayarın birbirleriyle herhangi bir kablo kullanmadan, radyo frekansları aracılığıyla yönlendiriciler ve/veya aracılar kullanarak haberleşmesini sağlarlar. Amerikan National Institute of Standards and Technology (NIST) ye göre, kablosuz ağlar 3 gruba ayrılabilirler [1]; Geniş Alan Kablosuz Ağlar (Wireless Wide Area Network- WWAN)), Kişisel Kablosuz Ağlar (Wireless Personal Area Network-WPAN), Yerel Kablosuz Ağlar (Wireless Local Area Network-WLAN). Geniş Alan Kablosuz Ağlar isminden de anlaşılabileceği gibi büyük bir alana yayılmış ve çok sayıda kullanıcısı olan bilgisayarlar topluluğunun kablosuz iletişim adaptörleri kullanarak birbirleriyle haberleşmesiyle oluşur. Kişisel Kablosuz Ağlar, küçük bir alan içerisindeki kişisel bilgisayarların birbirleriyle Bluetooth, RFID, IrDA gibi teknolojiler kullanarak haberleşmesini sağlar. Yerel Kablosuz Ağlar ise aynı alan (apartman, ofis, vb.) içerisinde bulunan birden fazla kullanıcının kablosuz bağlantı kurmasına olanak verirler.

Kablosuz ağlar çok farklı ortamlarda bilgi alışverişini sağlayabilmeleri sayesinde hemen her alanda kullanılabilirler. Ancak bu iletişim radyo dalgalarıyla sağlandığı için erişim noktaları arasındaki bilgi alışverişi dışarıdan gelebilecek tehditlere açıktır. Bu nedenle güvenlik kablosuz ağların beraberinde gelen en önemli sorun olarak önümüze çıkmaktadır.

2 Yapısız Ağlar

Yeni teknolojilerin ortaya çıkması ve yeni ihtiyaçlar duyulması sonucunda zamanla Yapısız Ağlar olarak adlandırılan yeni bir bilgisayar ağları tanımı oluşmuştur. Yapısız Ağlar, genelde belli bir alan içinde bulunan kullanıcı grubunun, aracı görevini gören kablosuz erişim noktalarına bağlanamadıklarında ya da bağlanmak istemediklerinde birbiriyle haberleşirken geçici olarak meydan getirdikleri ağlardır [2]. Bu yapılar özellikle fiziksel ya da teknolojik koşulların getirdiği sorunlar sebebiyle erişim noktalarına ulaşmanın mümkün olmadığı askeri ya da doğal felaket ortamlarında rahatlıkla uygulabilir oldukları için günümüzde oldukça yaygın bir şekilde kullanılmaktadır.

Yapısız Ağlar diğer kablosuz ağlarla aynı teknolojik ortamlarda çalışmalarına karşın, ihtiyaç duyduğu protokoller sebebiyle kendisine has özellikleri bünyesinde bulundurur [2, 3]. Yapısız ağlar öncelikle herhangi bir coğrafi ortamda kullanılabilecekleri için ağın içinde bulunan her bir bilgisayarın birbirleriyle iletişim kurarken aynı zamanda birbirlerine karşı erişim noktası/yönlendirici görevini de üstlenmeleri gerekebilir. Bu nedenle dinamik bir ağ topolojisine sahip olmalı ve özellikle ağın farklı noktalarının birbirleriyle iletişimleri esnasında hızlı bir şekilde bilgi

ulaşımını saglayabilmelidirler. Ayrıca erişim noktası, yönlendirici gibi yapıların geçerli olmadığı ortamlarda, ağı oluşturan birimler arasındaki hiyerarşik düzen ve güvenlik sorunları ağ üzerinde oluşturulacak yeni ve farklı düzenlemelere yol açacaktır. Bu arada Yapısız Ağın genelde taşınabilir bilgisayarlar ya da cep bilgisayarları gibi taşınabilir birimlerden oluşacağı düşünüldügünde, bütün bu işlemlerin hızlı bir şekilde tamamlanabilmesi için ihtiyaç duyulan gücün ve yeterliliğin sağlanması ayrı bir önem taşımaktadır [2, 3]. Aynı şekilde ağın farklı noktaları arasındaki mesafeler büyüdükçe bilginin en kısa yoldan ulaştırılabilmesi için gerekli olan iletişim altyapısının uygun ve hızlı bir şekilde kurulabilmesine ihtiyaç vardır. Bilgi, daha önce de belirtildiği gibi radyo dalgalarıyla, herkesin erişimine açık bir şekilde iletildiği için kablolu ağlarda uygulananlardan daha sıkı güvenlik protokollerinin oluşturulmasına gerek duyulmaktadır.

Yapısız Ağın sahip olduğu bu nitelikler, iş toplantılarından, konferanslara, savaş ortamından, doğal felaketlere kadar her tür zorlu koşulda kullanıbilmesini sağlarlar [3, 4]. Fakat, yukarıda belirtildiği gibi, aynı zamanda güvenlik, ağın içinde en kısa yolun en hızlı şekilde bulunması, bilginin hızla iletimi, güç kullanımı, kaynak kullanımı, servisin kalitesi ve ağın konfigurasyonu gibi problemler Yapısız Ağların beraberlerinde getirdikleri sorunlar olarak karşımıza çıkmaktadırlar [1].

3 Yapısız Ağlarda Güvenlik İhtiyaçları

Yapısız Ağlarda farklı kullanıcılar birbirleriyle iletişim sağlamak istediklerinde aynı sinyal alım menzilinde bulunan herhangi bir ya da birden çok birim bulunabilir. Bu nedenle öncelikle bu iletişimin yapılacağı birimler arasında bir tür kimlik denetimi yapılması ve iki tarafın da birbirlerinin kimliklerini onaylaması gerekebilir [5, 6]. Ayrıca bu sayede Yapısız Ağa sadece yetkili kişilerin erişimi sağlanır ve kötü niyetli birimlerin ağa giriş izni olan birimleri taklit ederek ağa erişimleri de engellenir.

Kimlik denetimden sonra Yapısız Ağlarda ihtiyaç duyulan ikinci özellik ise gizililiktir. Yani iletilen bilgiye sadece iletişimi gerçekleştiren taraflarca ulaşılabilmesinin sağlanmasıdır. Bu aynı zamanda ağa bağlı olan birimlerin gizliliklerinin de korunması anlamına gelir. Gizlilik özellikle askeri ve ticari ortamlarda kullanılan Yapısız Ağlarda bilginin saklanması, korunması, hızlı ve doğru bir şekilde iletilmesi yönünden de çok önemlidir. Ayrıca, ağın içindeki yönlendirme bilgilerinin de dışarıdan gelebilecek olası saldırılara karşı saklanması yani korunması gerekir [6,7].

Yapısız Ağlarda dikkat edilmesi gereken bir diğer konu, iletilen bilginin orijinal halinde herhangi bir değişiklik olmadan iletiyi alacak olan birime ulaştırılabilmesi, yani bilginin bütünlüğünün korunmasıdır. İletilen mesajın kötü niyetli birimler tarafından üzerinde oynama yapılmadan, silinmeden ya da ekleme yapılmadan alıcıya iletilmesidir.

Yapısız Ağlarda dikkat edilmesi gereken bir güvenlik ihtiyacı da transferi yapılan bir bilginin hem gönderen hem de alıcı tarafından inkar edilememesidir. Böylece bilgiyi gönderen gönderdiğini, bilgiyi alan da aldığını transfer tamamlandıktan sonra red edemezler. Bu özellik aynı zamanda bir şekilde ağa girmeyi başaran kötü niyetli birimlerin tespitine katkıda bulunur [7].

Bilginin ulaşılabilirliği ve sürekliliği de Yapısız Ağlarda sağlanması gereken bir özelliktir. Buradaki sürekliliğin anlamı, Yapısız Ağı oluşturan birimlerin ağın içinden ya da dışından gelebilecek olası tehditlere, dikkatsiz kullanımlara, yazılım hatalarına karşı durarak iletişimin ve ağın devamlılığının sağlanması demektir. Süreklilik hizmeti sayesinde, birimler, erişim yetkileri içinde olan bilgilere, hızlı ve güvenilir bir şekilde erişebilirler [6, 7].

Yapısız Ağlardaki diğer bir güvenlik ihtiyacı da birimlerin yetkilendirilmesidir. Yetkilendirme tanımı, ağa erişimi olan birimlerin her birinin erişim izinleri ve yetkilerinin hiyerarşik bir düzen içinde tanımlanması ve saklanmasının sağlanmasıdır [5, 6, 7]. Bu şekilde ağın içinde olan ve yetkisi dışında işlevlere kalkışan birimlerin veya dışardan gizlice erişim sağlayan kötü niyetli birimlerin yaratabilecekleri olası sorunlara karşı önlem alınması sağlanır [8, 9].

4 Yapısız Ağlarda Güvenlik Tehditleri

Tüm diğer ağlarda olduğu gibi Yapısız Ağlar da güvenlik saldırılarına karşı son derece duyarlıdırlar ve yaralanabilirlerdir. Yapısız kablosuz ağlarda hem diğer kablolu ve kablosuz ağlarda görülen güvenlik sorunları hem de Yapısız Ağların özelliklerinden kaynaklanan güvenlik sorunları ortaya çıkmaktadır [13].

Saldırı çeşitliliği değişik faktörlerden etkilenir. Bu faktörler aynı zamanda uygulanabilecek savunma mekanizmalarını da belirlemektedir. Saldırı çeşitlerini etkileyen bu faktörler genel olarak; Yapısız Ağ ortamları, iletişim katmanları ve saldırı düzeyleri olarak adlandırılabilir [13, 14].

Yapısız kablosuz ağların kendilerine özgü topolojileri, dağıtık işlem yöntemleri ve kaynak kısıtlamaları gibi özelliklerinin birçoğu yapısız ağlara yapılan saldırıları sınıflandırmak için kullanılabilir. Sınıflandırmayı yaparken saldırının davranışına (etken veya edilgen), saldırının kaynağına (içerden veya dışardan), saldırı kaynağının kapasitesine (kablosuz veya kablolu) ve saldırgan sayısına (tek veya çoklu) bakılarak sınıflandırma yapılabilir [12, 13].

Yapısız Ağlarda bilgi veya iletilerin normal akışından kopmalarına sebep olan saldırı yöntemleri değişiklik, engelleme, kesme veya fabrikasyon isimleri altında sınıflandırılabilir. Bazen saldırganlar bu saldırı

yöntemlerinin de birden fazlasını birlikte kullanarak daha etkin saldırılarda bulunabilirler [13].

İleti değişikliği saldırı türlerinde, saldırgan dolaşım iletilerini değiştirmekte, böylece iletinin bütünlüğünü bozmaktadır. Yapısız Ağlarda serbest dolaşım ve kendi kendini yönlendirme özellikleri bulunduğundan, bu tip iletilerinin bozulması ciddi sıkıntılar yaratmaktadır. Bu tip saldırılarda değişik yöntemler uygulanmaktadır. Saldırgan orijinal paketleri alıp yanlış alıcılara yönlendirilmelerini sağlayabileceği gibi, başka birimlerin kimliğini kullanarak yanlış paketler gönderebilmektedir. Tüm bu tür saldırıların ortak noktası ise ağ üzerindeki trafiği ve dolayısıyla maliyetleri artırmalarıdır [13, 14].

Engelleme tarzı saldırılarda genel olarak saldırganlar kendilerine gönderilmeyen ileti paketlerine ulaşmaya çalışmaktadırlar. Saldırgan bu paketleri elde ettikten sonra bunlar üzerinde tüm ağın bütünlüğü ve güvenliğini bozabilecek ileti değişikliklerini yapabilmektedir [13, 14].

Fabrikasyon saldırılarında saldırganlar varolan iletileri değiştirme veya kesme yerine kötü niyetli kendi paketlerini yaratarak ağ içinde kaos ve düzensizliğe neden olabilirler. Büyük miktarda paketler göndererek ağın aşırı yoğunlaşmasına ve iletim hızının azalmasına sebep olurlar. Bu tip saldırı türleri genel olarak yapısız kablosuz ağlara özgü saldırılardır [13, 14].

Saldırganlar ağın normal işleyişini rahatsız etmek veya durdurmak için yukarıdaki yöntemlerden başka, hedef düğüme gereksiz ve büyük miktarda paket göndererek düğümün sürekli meşgul olmasını sağlar ve başka iletiler ve paketler alabilmesini engeller. Bu tip saldırılar genel olarak boğma (flooding) saldırıları olarak adlandırılmaktadırlar [14].

5 Yapısız Ağlarda Güvenlik Tedbirleri

Saldırılardan korunma bilgisayar ağlarında en önemli güvenlik safhalarından biridir. Korunma mekanizması olarak adlandırılan bu işlevin amacı genelde dışarıdan gelecek olan saldırılara karşı ağın bütünlüğünün sağlanması, çalışılabilirliğinin devam ettirilmesidir. Bu amaçla alınabilecek ilk önlem kimlik doğrulamanın düzgün bir şekilde, kriptografi kullanılarak ağa uygulanmasıdır. Ancak Yapısız Ağlarda bunu yapabilmek Kablolu Ağlara göre daha zordur, çünkü ortada sabit erişim noktaları ve yönlendiriciler yoktur. Bu nedenle Yapısız Ağlarda bu konseptlere uyan özel kimlik doğrulama protokolleri ve daha fazla güvenlik içeren yönlendirme protokolleri kullanılmaktadır. Buradaki zorluk Yapısız Ağlarda Kablolu Ağlardan farklı olarak güvenlik anahtarlarının kullanılmasıyla gerçekleştirilen kimlik denetimlerinin uygulanmasında anahtarları sağlayacak merkezi bir otorite olmamasından kaynaklanmaktadır. Bu sebeple farklı metodlar kullanılarak anahtar değişimi yapılması gerekmektedir (her bir birimin diğer bir birime merkezi otorite olarak anahtar sağlaması, bir birimin yakındaki başka bir birimle usta-çırak ilişkisi kurması, arkadaş tavsiyesi vb.) [9, 10, 11].
Yapısız Ağlarda saldırılardan korunma dışında uygulanabilecek olan bir diğer güvenlik mekanizması da tespit mekanizmasıdır. Bu amaçla kullanılabilen İzinsiz Giriş Tespit Sistemi (Intrusion Detection System-IDS) ağ içindeki trafiği izleyerek ağın içindeki kötü birimleri tespit edebilmektedir. İyi bir IDS gerçek zamanlı olarak ağa yapılan saldırıları tespit edebilmeli ve karşı koyabilmeli, değişen saldırı metotlarına karşı yeni önlemler alarak kendini yenileyebilmelidir. Aynı zamanda ağda bulunan izinsiz ve yetkisiz birimleri yakalayabilmelidir [11, 12].

Bir IDS'in etkinliği çalıştığı ağ üstünde toplamış olduğu bilginin kalitesiyle doğru orantılıdır. Bunun gerçekleşmesi için hem alıcı birimde hem de gönderici birimde yapılan işlevlerle ilgili bilgi toplanması ile olur. Burada kastedilen birimlerin ağda gerçekleştirdiği tüm işlemlerin kaydının tutulması ve bu kayıtlardan yola çıkılarak birimlerin kullanıcı karakteristiklerinin tanımlanması ve bu karakteristiklerin iyi niyetli olup olmadıklarına bakılmasıdır [12]. Burada sorun, bu tip bir IDS'de karar mekanizmasında bir sistem yetkilisine ihtiyaç duyulmasıdır. Yapısız Ağlar da bağımsız birimlerden oluştuğu için bu tarz bir tespit sisteminin sağlıklı sonuçlar vermesi mümkün değildir. Bu nedenle birçok araştırmacı ağdaki bazı birimlerin güvenlik duvarlarının ve sunucuların yerini alabilecekleri yeni yöntemler önermişlerdir [15, 16].

Bunlardan en yaygın olanı her bir birimin diğer birimlerin arasında gerçekleşen iletimleri alabilme kapasitesi olduğundan bu iletimleri de kayıt altına alabilme ihtimali üzerine hazırlanan tespit sistemidir. Bu sistemin çalışabilmesi ancak bahsedilen birimlerin birbirlerinin menzilleri içinde olması durumunda mümkündür [15, 16, 17, 18].

Diğer bir yöntem de ajan teknolojileri (küçük akıllı programlar) kullanılarak gerçekleştirilebilecek olan yaklaşımdır. Bu tespit sisteminde her birim kendi ajanını ağın içindeki tüm birimlere göndererek her bir birimin gerçekleştirdiği trafiği takip etmesini sağlar. Bu sistemde sorun bu programların kimlik denetimlerinin yapılmasının güçlüğüdür [19].

Tespit sistemlerinde analiz yapılırken genellikle kötü kullanım ya da yetkisiz kullanım diye adlandırılan inceleme teknikleri kullanılır. Kötü kullanım tekniğinde ağın içindeki normal trafiğin genel özellikleri ile ilgili olarak çıkartılan bir profille gerçek zamanlı trafik karşılaştırılarak ortamda bir saldırının olup olmadığına bakılır. Bu sistemde ağın içindeki hareketliliğin zamanla değişmesi göz önüne alınarak sistemin eğitilmesi gerekir. Yetkisiz kullanımdaysa daha önceden hazırlanmış ve veritabanında saklanan saldırı profilleri gerçek zamanlı olarak anlık ağ trafiği ile kıyaslanarak saldırı olup olmadığı anlamaya çalışılır [19]. Yapısız

Ağlarda genellikle kötü kullanım tekniği yetkisiz kullanım tekniğine tercih edilir, çünkü Yapısız Ağlar henüz yeni olduğu için saldırı profillerini ayırt edebilmek çok zordur [17, 18, 19, 20].

Yapısız Ağların yukarıda da belirtilen genel zorluklarından yola çıkarak tespit sistemleri için birçok değişik görüşler ortaya atılmıştır. Bu görüşlerde bazı araştırmacılar yönlendirici görevi gören birimlerin üzerinden tespit yapılmasını teklif ederken [15], diğerleri de her bir birimin kendi kendisine analizler yapmasını desteklemişlerdir [21, 24, 25]. Bunların bazılarında iletiyi gönderen birimin ileti yolu, komşu birimler, ileti zamanları gibi bilgileri toplarken alıcı birimin herhangi bir şeye karışmasına gerek görülmemiştir [21, 22, 23].

Tespit sistemlerinin genel problemleri olan yanlış alarmlar özellikle kötü kullanım tekniği ile analiz yapıldığında çok yaygın olarak karşımıza çıkarlar. Yanlış alarm, tespit sisteminin normal bir kullanımı kötü kullanım olarak betimlemesiyle oluşur. Bu sorun Yapısız Ağlarda çok yaygın bir problemdir, çünkü normal ve kötü kullanım profillerinin kolayca tanımlanabilmesi mümkün değildir. Bu nedenle, birimlerde Yapısız Ağ trafik bilgileri mümkün oldukça yoğun olarak kayıt altına alınarak, daha fazla bilgi, daha kesin analizler mantığıyla çalışan IDS'lere ihtiyaç vardır [21, 22, 23, 24, 25].

6 Sonuç

İzinsiz Giriş Tespit Sistemi (Intrusion Detection System-IDS) Yapısız Ağlarda kullanılması oldukça zor olan bir sistem olmasına karşın iyi tasarlanmış bir IDS yukarıda tanımı yapılan birçok aktif saldırı türlerine karşı durabilir. Burada kastedilen IDS, ağa erişmiş olan saldırganın bulunduğu yer, yaptığı işlemler, yerine geçtiği birimin karakteristik özelliklerinin karşılaştırılması gibi farklı işlevleri inceleyerek doğru kararı verebilmesidir. Elbette burada doğru bir tasarım mantığı oluşturmak çok önemlidir. Burada düşünülen, Yapısal Ağlarda olası saldırıların önceden önlenmesinin çok zor olması nedeniyle, ağa erişimi başarmış olan yetkisiz birimlerin tesbitine yönelik bir IDS geliştirebilmektir.

7 Kaynaklar

[1] T. Karygiannis and L. Owens, "Wireless Network Security 802.11," Bluetooth and Handheld Devices, NIST Publication (800-48), Nov., 2002.

[2] J. Al-Jaroodi, "Security Issues in Wireless Mobile Ad Hoc Networks at the NetworkLayer," Technical Report TR02-10-07, Computer Science and Engineering, University of Nebraska-Lincoln, Nov., 2002.

[3] K. Rafique, "A Survey of Mobile Ad Hoc Networks," Columbia University Student Project Report, 2002.

[4] http://www.cs.ucsb.edu/projects/wireless/research desc/network/eroyer.shtml, "A Brief Description of the Wireless Project," CISE Wireless Project, 2002.

[5] L. Buttyan and J. –P. Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks," Mobile Computing and Communications Review, Vol. 7, Number 1, pp. 74-94, Jan., 2003.

[6] P. Albers, O. Camp, J. –M. Percher, B. Jouga, L. Mé, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," In Proc. of the First International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, Apr., 2002.

[7] S. Maki, "Security Fundamentals in Ad-hoc Networking," Seminar Paper, Seminar on Internetworking, Helsinki University of Technology, 2000.

[8] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks," 1999 AT&T Software Symposium, Sept., 1999.

[9] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies," in Proc. of The 23rd International Conference on Distributed Computing Systems (ICDCS), pp. 478-489, May 19-22, 2003.

[10] M. King, "Security Lifecycle- Managing the Threat," GSEC Practical vo1. 3, Jan., 2002.

[11] S. Capkun, J. -P. Hubaux, and L. Buttyan, "Mobility Helps Security in Mobile Ad Hoc Networks," in Proc. of MobiHoc'03, Annapolis, Maryland, USA, pp. 46-56, Jun. 1-3, 2003.

[12] D. Balfanz, D. Smetters, P. Stewart, and H. Wong, "Talking to Strangers- Authentication in Ad Hoc Wireless Networks," In Proc. of the 9th Annual Network and Distributed System Security Symposium (NDSS), San Diego, California, Feb. 6-8, 2002.

[13] J. P. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," in Proc. of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHOC 2001, pp. 146-155, Oct. 4-5, 2001.

[14] S. Maki, "Security Fundamentals in Ad-hoc Networking," Seminar Paper, Seminar on Internetworking, Helsinki University of Technology, 2000.

[15] I. Stamouli, "Real-time Intrusion Detection for Ad hoc Networks," Technical Report, Computer Science

Department, University of Dublin, Trinity College, Dec. 10, 2003.

[16] S. Buchegger and J-Y. L. Boudec, “IBM Research Report: The Selfish Node - Increasing Routing Security for Mobile Ad Hoc Networks,” RR 3354, 2001.

[17] K. Paul and D. Westhoff, “Context Aware Detection of Selfish Node in DSR based Ad-hoc Network,” IEEE Global Telecommunications Conference (2002), pp. 178-182, Taipei, Taiwan, Nov. 17-21, 2002.

[18] O. Kachirski and R. Gupta, “Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks,” IEEE Workshop on Knowledge Media Networking (KMN'02), pp. 153-160, Kyoto, JAPAN, Jul. 10 - 12, 2002.

[19] A. Vattikonda, R. K. Gampa, V. K. Isukapalli, and V. R. Kakarlapudi, “Intrusion Detection In Wireless Networks,” Term Paper, Department of Computer Science, The University of Kentucky, 2003.

[20] A. V. Meier, “IDS in Ad Hoc Networks,” Seminar Paper, Hauptseminar Ad Hoc Networks, Technische Universität München, Institut für Informatik, Nov., 2003.

[21] F. H. Wai, Y. N. Aye, and N. H. James, “Intrusion Detection in Wireless Ad-Hoc Networks,” Term Paper, School of Computing, National University of Singapore, 2003.

[22] W. W. Cohen, “Fast Effective Rule Induction,” In Proc. of 12th International Conference on Machine Learning, pp. 115-123, Morgan Kaufmann, 1995.

[23] T. Joachims, “SVM Light Support Vector Machine,”http://svmlight.joachims.org, Sept., 2004.

[24] M. Just, E. Kranakis, and T. Wan, “Resisting Malicious Packet Dropping in Wireless Ad-Hoc Networks,” In Proc. of 2nd Annual Conference on Ad hoc Networks and Wireless (ADHOCNOW'03), Montreal, Canada, Oct. 09-10, 2003.

[25] B.Awerbuch, D. Holmer, C. N. -Rotaru, and H. Rubens, “An on-demand secure routing protocol resilient to byzantine failures,” In ACM Workshop on Wireless Security (WiSe'02), pp. 21-30, Atlanta, Georgia, Sept., 2002.