**Slika 1**

1.Alisa salje Bobu indetifikacionu poruku (“Ja sam Alisa”) I neku random generisanu vrednost Ra  
2.Bob prima od Alise poruku I salje svoju random generisanu vrednost Rb,zatim sifruje sa simetricnim algoritmom random generisanu vrednost Alise-Ra sa zajednickim kljucem Kab

3.Alisa prima Rb I desifruje poruku dobijenu od Boba sa simetricnim kljucem Kab I dobija svoje Ra na osnovu koga verifikuje Boba.Zatim sifruje sa simetricnim kljucem Kab bobovu random generisanu vrednost Rb.

4.Bob prima sifrat od Alise desifruje sa zajednickim kljucem Kab I dobija Rb I verifikuje Alisin identitet.

U ovom protokolu postignuta je obostrana autentifikacija ali se otvara mogucnost za Man in the Midlle napad.  
  
  
**Slika 2**U ovom protokolu Trudi pokusava da izvrsi napad predstavljajuci se pod laznim indentitetom pred Bobom kao Alisa

1.Trudi se predstavlja Bobu “Ja sam Alisa” I generise neko svoje Ra-izazov koji zatim salje Bobu.

2.Bob salje svoju random generisanu vrednost Rb,zatim sifruje sa simetricnim algoritmom Alisino(Trudi) Ra sa zajednickim kljucem Kab.Trudi ne znajuci zajednicki kljuc Kab nije u mogucnosti da desifruje poruku I zato otvara novu paralelnu komunikaciju.

3.U novoj paralelnoj komunikaciji ponovo se predstavlja Bobu “Ja sam Alisa” I salje mu njegovo Rb-izazov koji salje Bobu umesto Ra.

4.Bob ne znajuci da mu je Alisa poslala njegov parametar kreira neko Rc random generisani parametar I sifruje simetricnim algoritmom svoje Rb sa simetricnim kljucem Kab I sifrat salje Trudi.

5.U petom koraku Trudi verifikuje Boba i vraca se na prvu komunikaciju salje Bobu sifrat E(Rb,Kab) sifrovano sa simetricnim algoritmom I sa zajednickim kljucem I njegovim parametrom koje je on sifrovao I uspeva da prevari Boba.Bob ne znajuci da je to Lazna Alisa(Trudi) verifikuje Alisu I potvrdjuje njen indentitet ne znajuci da je sa druge strane protokola Trudi.

**MODIFIKACIJA:**

Da bi se onemogucio napad na protokol sa Slike 2 od strane Trudi neophodno je uvesti neke teksutualne parameter koji ce oznacavati identitet Boba I indentitet Alise.Da li ovi parametri mogu da pomognu u protokolu? Odgovor je DA! U prvom koraku bi Alisa poslala poruku Ja sam Alisa I generisala svoju random vrednost Ra Bob bi odgovorio genersisanjem svoje vrednosti Rb I sifrovanjem parametra koji potvrdjuje negjov indentitet (tekst “Bob”) sa Alisinim Ra i zajednickim kljucem –simetricnim kljucem Kab.Alisa bi desifrovala sifrat dobijen od Boba I time dobila Ra koje je poslala Bobu I parametar “Bob” koji pomaze u indentifikaciji da je to zaista Bob.Time bi se onemogucilo da se Trudi prestavi kao Bob ili Alisa I tako izvrsi napad.Time je sprecen MIM napad.U sledecem koraku Alisa sifrtuje Bobovu random vrednost Rb,parametar Alisa sa simetricnim kljucem Kab.Bob vrsi desifrovanje zajednickim kljucem Kab I dobija Rb I parameter Alisa na osnovu koga verifikuje Alisu I ostvarena je uzajamna autentifikacija.Ovaj protokol nije podlezan MIM napadu I ponovnom reprodukovanju poruka cak sta vise ovaj protokol je siguran.

**TACKA 3**

Ukoliko bi nakon predlozene modifikacije zeleli da ubacimo I vremenski pecat morali bi da izvrsimo niz promena pocev od toga da bi Ra ili Rb zamenili sa T odnosno vremenskim parametrom koji je karakteristican za koriscenje vremenskog pecata.Izbacili bi parametre”Alisa” I parametar “Bob” I uveli nove parametre digitalno potpisivanje I sifrovanje sa javnim I privatnim kljucevima tj koristili dva para kljuceva I skratili bi za 1 fazu.Ukratko protokol bi izlgedao ovako:

1.Alisa salje Bobu poruku ja sam Alisa,I salje mu neku vremensku oznaku T I kljuc sesije K digitalno potpisano sa svojim privatnim kljucem.Zatim ceo sifrat sifruje sa Bobovim javnim kljucem.

2.Bob prima poruku od Alise vrsi desifrovanje simetricnog algoritma svojim privatnim kljucem I dobija digitalno potpisanu poruku [T,K] koji desifruje sa Alisinim javnim kljucem I dobija vrednost vremenskog parametra T I sesijskog kljuca K.Zatim salje Alisi digitalno potpisan vremenski parametar T-inkrement ondnosno uvecano za 1,T+1 radi osvezavanja I sprecavanja napada I sesijski kljuc K potpisan sa svojim privatnim kljucem. I na kraju vrsi sifrovanje cele vrednosti koju je potpisao sa Alisinim javnim kljucem.I na kraju protokola na identican nacin Alisa verifikuje Boba. I ostvarena je obostrana autentifikacija.Ovaj protokol je siguran nema prostora za ostvarivanje MIM napad.Ovaj protokol je potpuno bezbedan.